

1 CHRISTOPHER GRIVAKES

2 cg@agzlaw.com

3 DAMION ROBINSON

4 dr@agzlaw.com

AFFELD GRIVAKES LLP

5 2049 Century Park East, Suite 2460

6 Los Angeles, CA 90067

7 Telephone: 310.979.8700

Facsimile: 310.979.8701

8 Attorneys for Plaintiff ROBERT ROSS

9  
10  
11 THE UNITED STATES DISTRICT COURT  
12 FOR THE NORTHERN DISTRICT OF CALIFORNIA

13  
14 ROBERT ROSS,

15 Plaintiff,

16 v.

17 AT&T MOBILITY, LLC, ONE  
18 TOUCH DIRECT, LLC, and ONE  
19 TOUCH DIRECT- SAN ANTONIO,  
LLC,

20 Defendants.  
21  
22  
23  
24  
25  
26  
27  
28

Case No. 4:19-cv-6669

**FIRST AMENDED COMPLAINT**

**DEMAND FOR JURY TRIAL**

1       **I.     NATURE OF THE ACTION**

2           1.     This action arises out of AT&T’s failure to protect the sensitive and  
3 confidential account data of its mobile service subscriber, Robert Ross, resulting in  
4 massive violations of Mr. Ross’s privacy, the compromise of his highly sensitive  
5 personal and financial information, and the theft of more than \$1 million.

6           2.     AT&T is the country’s largest mobile service provider. Tens of  
7 millions of subscribers entrust AT&T with access to their confidential information,  
8 including information that can serve as a key to unlock subscribers’ highly  
9 sensitive personal and financial information.

10          3.     Recognizing the harms that arise when mobile subscribers’ personal  
11 information is accessed, disclosed, or used without their consent, federal and state  
12 laws require AT&T to protect this sensitive information.

13          4.     AT&T also recognizes the sensitivity of this data and promises its 150  
14 million mobile subscribers that it will safeguard their private information – and  
15 particularly their data-rich SIM cards – from any unauthorized disclosure. AT&T  
16 promises it “will protect [customers’] privacy and keep [their] personal  
17 information safe” and that it “will not sell [customers’] personal information to  
18 anyone, for any purpose. Period.” AT&T repeatedly broke these promises.

19          5.     In an egregious violation of the law and its own promises, and despite  
20 advertising itself as a leader in technological development and as a cyber security-  
21 savvy company, AT&T breached its duty and promise to Mr. Ross to protect his  
22 account and the sensitive data it contained. AT&T failed to implement sufficient  
23 data security systems and procedures, instead allowing third parties to gain  
24 unauthorized access to Mr. Ross’s AT&T account in order to steal from him.

25          6.     AT&T’s actions and conduct were a critical factor in causing  
26 significant financial and emotional harm to Mr. Ross and his family. But for AT&T  
27 employees’, representatives’ and agents’ unauthorized access to Mr. Ross’ account,  
28 and failure to protect Mr. Ross through adequate security and oversight systems

1 and procedures, Mr. Ross would not have had his personal privacy repeatedly  
2 violated and would not have been a victim of SIM swap theft.

3 7. Mr. Ross brings this action to hold AT&T accountable for its  
4 violations of federal and state law, and to recover for the grave financial and  
5 personal harm suffered by Mr. Ross and his family as a direct result of AT&T's acts  
6 and omissions, as detailed herein.

## 7 **II. THE PARTIES**

8 8. Plaintiff Robert Ross is, and at all relevant times was, a resident of  
9 California. Mr. Ross currently resides in San Francisco, California.

10 9. Mr. Ross was an AT&T mobile customer at all times relevant to this  
11 Complaint. He purchased a mobile phone plan from AT&T in San Francisco,  
12 California in 2007 for personal use, was an active, paying AT&T mobile subscriber  
13 at all times relevant to the allegations in this Complaint, and his business  
14 relationship was directly with AT&T at all relevant times.

15 10. Defendant AT&T Mobility, LLC (hereinafter, "AT&T") is a Delaware  
16 limited liability corporation with its principal office or place of business in  
17 Brookhaven, Georgia. AT&T "provides nationwide wireless services to consumers  
18 and wholesale and resale wireless subscribers located in the United States or U.S.  
19 territories" and transacts or has transacted business in this District and throughout  
20 the United States. It is the second largest wireless carrier in the United States, with  
21 more than 153 million subscribers, earning \$71 billion in total operating revenues  
22 in 2017 and \$71 billion in 2018. As of December 2017, AT&T had 1,470 retail  
23 locations in California.<sup>1</sup>

24 11. AT&T provides wireless service to subscribers in the United States.  
25 AT&T is a "common carrier" governed by the Federal Communications Act  
26 ("FCA"), 47 U.S.C. § 151 *et seq.* AT&T is regulated by the Federal

---

27  
28 <sup>1</sup> "About Us," AT&T, available at <https://engage.att.com/california/about-us/>. This URL was last accessed on October 15, 2019.

1 Communications Commission (“FCC”) for its acts and practices, including those  
2 occurring in this District.

3 12. AT&T Inc., AT&T’s parent company, acknowledged in its 2018  
4 Annual Report that its “profits and cash flow are largely driven by [its] Mobility  
5 business” and “nearly half of [the] company’s EBITDA (earnings before interest,  
6 taxes, depreciation and amortization) come from Mobility.”<sup>2</sup>

7 13. Defendant One Touch Direct, LLC (“One-Touch Direct”) is a Florida  
8 Corporation with its principal place of business in Tampa, Florida. Plaintiff is  
9 informed and believes and thereon alleges that AT&T contracted with One-Touch  
10 Direct to provide call center services for AT&T’s mobile phone customers.

11 14. Defendant One Touch Direct - San Antonio, LLC (“One-Touch  
12 Direct-SA”) is a Florida Corporation with its principal place of business in Tampa,  
13 Florida. Plaintiff is informed and believes and thereon alleges that One-Touch  
14 Direct-SA is a subsidiary of One Touch Direct - SA and the employer of the  
15 customer service representative(s) who executed the remote SIM swap on  
16 Plaintiff’s mobile phone.

17 15. At all relevant times, One Touch Direct and One Touch Direct-SA  
18 were AT&T’s authorized representatives and agents and performed services for  
19 AT&T which were within the usual course of AT&T’s business.

20 16. At all relevant times, AT&T dictated and controlled the manner and  
21 means by which One Touch Direct and One Touch Direct-SA performed their  
22 services for AT&T. On information and belief, AT&T entered into a master  
23 services agreement with One Touch Direct which governed the terms and condition  
24 of AT&T’s relationship with One Touch Direct and its subsidiaries such as One  
25 Touch Direct-SA, and which required the One Touch entities to strictly adhere to  
26 AT&T’s guidelines, protocols, policies, and procedures relating to customer  
27

---

28 <sup>2</sup> *Id.*

1 service, including those relating to SIM swaps. Furthermore, AT&T controlled the  
2 security measures it implemented across its entire network operation (including its  
3 own call centers and third-party call centers), as well as the data accumulated  
4 across the entire network, to monitor, detect and prevent unauthorized SIM swaps.

5 17. At all relevant times, One Touch Direct and One Touch Direct-SA  
6 employees identified themselves to Mr. Ross as “AT&T” rather than One Touch  
7 Direct (at AT&T’s direction), had full access to and use of the AT&T customer  
8 database which enabled them to perform customer service functions (including  
9 SIM swaps), did not disclose that they were employed by One Touch Direct, and  
10 were in essence *de facto* employees of AT&T.

### 11 **III. JURISDICTION AND VENUE**

12 18. This Court has jurisdiction over this matter under 28 U.S.C. § 1331  
13 because this case arises under federal question jurisdiction under the Federal  
14 Communications Act (“FCA”). The Court has supplemental jurisdiction under 28  
15 U.S.C. § 1367 over the state law claims because the claims are derived from a  
16 common nucleus of operative facts. The Court also has jurisdiction over this  
17 action pursuant to 28 U.S.C. § 1332 because Mr. Ross is a citizen of a different  
18 state than AT&T, One Touch Direct, and One Touch Direct-SA.

19 19. This Court has personal jurisdiction over AT&T and its contractors  
20 One Touch Direct and One Touch Direct-SA because AT&T purposefully directs its  
21 conduct at California, transacts substantial business in California (including in this  
22 District), has substantial aggregate contacts with California (including in this  
23 District), engaged and is engaging in conduct that has and had a direct, substantial,  
24 reasonably foreseeable, and intended effect of causing injury to persons in  
25 California (including in this District), and purposely avails itself of the laws of  
26 California. AT&T had more than 33,000 employees in California as of 2017, and  
27  
28

1 1,470 retail locations in the state.<sup>3</sup> Mr. Ross purchased his AT&T mobile plan in  
 2 California, visited AT&T retail locations in California, and was injured in  
 3 California by the acts and omissions alleged herein.

4 20. In accordance with 28 U.S.C. § 1391, venue is proper in this District  
 5 because a substantial part of the conduct giving rise to Mr. Ross' claims occurred  
 6 in this District and Defendant transacts business in this District. Mr. Ross  
 7 purchased his AT&T mobile plan in this District and was harmed in this District,  
 8 where he resides, by the acts and omissions of Defendants, as detailed herein.

#### 9 **IV. ALLEGATIONS APPLICABLE TO ALL COUNTS**

10 21. As a telecommunications carrier, AT&T is entrusted with the sensitive  
 11 mobile account information and personal data of millions of Americans, including  
 12 Mr. Ross' confidential and sensitive personal and account information. AT&T's  
 13 duties to safeguard customer information are non-delegable to any other entity,  
 14 including its third-party call center service providers such as the One Touch Direct  
 15 entities.

16 22. Despite its representations to its customers and its obligations under  
 17 the law, AT&T has failed to protect Mr. Ross' confidential information. In October  
 18 2018, AT&T employees, representatives and agents obtained unauthorized access  
 19 to Mr. Ross' AT&T mobile account, viewed his confidential and proprietary  
 20 personal information, and transferred control over Mr. Ross' AT&T mobile  
 21 number and service from Mr. Ross' phone to a phone controlled by third-party  
 22 hackers. The hackers then immediately utilized their control over Mr. Ross'  
 23 AT&T mobile number—control secured with necessary and direct assistance from  
 24 AT&T employees, representatives and agents—to access and take control of his  
 25 personal and digital finance accounts and steal \$1 million from Mr. Ross.  
 26  
 27

---

28 <sup>3</sup> “About Us,” AT&T California, *supra* at 1.

1           23. This type of telecommunications account hacking behavior is known  
2 as “SIM swapping.”

3           **A. SIM Swapping is a Type of Identity Theft Involving the Transfer**  
4           **of a Mobile Phone Number**

5           24. Mr. Ross was the victim of an unauthorized “SIM swap” on October  
6 26, 2018.

7           25. A “SIM swap” is a relatively simple scheme, wherein a hacker gains  
8 control of a victim’s mobile phone number and service in order to intercept  
9 communications, including text messages, intended for the victim. The hackers  
10 then use that phone number as a key to access and take over the victim’s digital  
11 accounts, such as email, file storage, and financial accounts.

12           26. Most mobile phones, including the iPhone owned by Mr. Ross at the  
13 time of his SIM swap, have an internal SIM (“subscriber identity module”) card. A  
14 SIM card is a small, removable chip that allows a mobile phone to communicate  
15 with the mobile carrier’s network and the carrier to know what subscriber account  
16 is associated with that mobile phone. The connection between the mobile phone  
17 and the SIM card is made through the carrier, which associates each SIM card with  
18 the physical phone’s IMEI (“international mobile equipment identity”), which is  
19 akin to the mobile phone’s serial number. Without an activated SIM card and  
20 effective SIM connection, a mobile phone typically cannot send or receive calls or  
21 text messages over the carrier network. SIM cards can also store a limited amount  
22 of account data, including contacts, text messages, and carrier information, and that  
23 data can help identify the subscriber.

24           27. The SIM card associated with a mobile phone can be changed. If a  
25 carrier customer buys a new phone that requires a different sized SIM card, for  
26 example, the customer can associate his or her account with a new SIM card and  
27 the new phone’s IMEI by working with their mobile carrier to effectuate the  
28 change. This allows carrier customers to move their mobile number from one

1 mobile phone to another and to continue accessing the carrier network when they  
2 switch mobile phones. For a SIM card change to be effective, the carrier is  
3 required by law to authenticate that the change request is legitimate and actualize  
4 the change. AT&T allows its employees, representatives and agents to conduct  
5 SIM card changes for its customers remotely or in its retail stores, and does so  
6 numerous times daily with inadequate protections against unauthorized SIM  
7 swaps.

8         28. An unauthorized SIM swap refers to an illegitimate SIM card change.  
9 During a SIM swap attack, a carrier representative switches the SIM card number  
10 associated with the victim's mobile account from the victim's phone to a phone  
11 controlled by a hacker. This literally re-routes the victim's mobile phone service  
12 — including any incoming data, texts, and phone calls associated with the victim's  
13 phone — from the victim's physical phone to a physical phone controlled by the  
14 hacker. The hacker's phone then becomes the phone associated with the victim's  
15 carrier account, and the hacker receives all of the text messages and phone calls  
16 intended for the victim.<sup>4</sup> Simultaneously, the victim's mobile phone loses its  
17 ability to connect to the carrier network and displays “No Service”.

18         29. Once hackers are given control over the victim's phone number, they  
19 can immediately use that control to access and take complete control of the  
20 victim's personal online accounts, such as email and banking accounts, through  
21 exploiting password reset links and codes sent via text message to the now-hacker-  
22 controlled-phone or the two-factor authentication processes associated with the  
23 victim's digital accounts. Two-factor authentication allows digital accounts to be  
24

---

25 <sup>4</sup> As described by federal authorities in prosecuting SIM swap cases, SIM swapping enables  
26 hackers to “gain control of a victim's mobile phone number by linking that number to a  
27 subscriber identity module (‘SIM’) card controlled by [the hackers]—resulting in the victim's  
28 phone calls and short message service (‘SMS’) messages being routed to a device controlled by  
[a hacker].” *United States of America v. Conor Freeman, et al.*, No. 2:19-cr-20246-DPH-APP  
(E.D. Mich. Filed Apr. 18, 2019) (hereafter, “Freeman Indictment”) (attached hereto as Exhibit  
A), ECF. No. 1 at ¶ 3.



1 accessed without a password or allows the account password to be changed. One  
2 common form of two-factor authentication enabled, allowed, and used by AT&T  
3 itself is through text messaging. Rather than enter a password, the hacker requests  
4 that a password reset link or code be sent to the mobile phone number associated  
5 with the victim's online account which AT&T makes possible. Because the hacker  
6 now controls the victim's phone number, the reset code is sent to the hacker. The  
7 hacker can then log into, and change the password for, the victim's account,  
8 allowing the hacker to access and take complete control of the contents of the  
9 account.<sup>5</sup>

10 30. Therefore, obtaining access to and control over a victim's mobile  
11 phone service is the central part of breaking into the victim's other online accounts,  
12 such as email services or financial accounts. The sole reason for the fraudulent  
13 SIM swap is for the hackers to take control of the victims' financial and online  
14 accounts that would not otherwise be accessible. A SIM swap is an extremely high-  
15 risk transaction, as it directly enables the hacker to take control of a victim's life.

16 31. The involvement of a SIM swap victim's mobile carrier is critical to  
17 an unauthorized SIM swap. In order for an unauthorized SIM swap to occur and  
18 for a SIM swap victim to be at any risk, the carrier must pro-actively and  
19 intentionally activate the SIM card in the hacker's phone, which simultaneously  
20 results in the SIM card in the victim's phone to be deactivated. At that point, the  
21 victim's phone will display "No Service" as their phone can no longer connect to  
22 the carrier's network.

23 32. Upon information and belief, in Mr. Ross's case, not only did AT&T  
24 employees, representatives and agents access his account without authorization,

---

25 <sup>5</sup> See, e.g., *Id.* at ¶ 4 ("Once [hackers] had control of a victim's phone number, it was leveraged  
26 as a gateway to gain control of online accounts such as the victim's email, cloud storage, and  
27 cryptocurrency exchange accounts. Sometimes this was achieved by requesting a password-reset  
28 link be sent via [text messaging] to the device control by [hackers]. Sometimes passwords were  
compromised by other means, and [the hacker's] device was used to received two-factor  
authentication ('2FA') message sent via [text message] intended for the victim.").

1 they also changed his SIM card number to a phone controlled by hackers, who then  
2 immediately used that control to steal from Mr. Ross and access sensitive personal  
3 information.

4 **B. AT&T Facilitated Unauthorized Access to Mr. Ross' AT&T**  
5 **Account and Gave Control of His Account to Hackers**

6 33. AT&T employees, representatives and agents accessed Mr. Ross'  
7 AT&T mobile account without his authorization, obtained his confidential and  
8 proprietary personal information, and gave complete control of his mobile service  
9 to hackers – all without Mr. Ross' knowledge or consent. Those hackers then  
10 immediately used their control over Mr. Ross' mobile phone number to access and  
11 take control of his sensitive and confidential information and accounts and steal  
12 more than \$1 million from him and access sensitive personal information such as  
13 passports, drivers' licenses and birth certificates.

14 34. On October 26, 2018 at approximately 6:00 PM PT, Mr. Ross began  
15 receiving notifications that someone was attempting to withdraw currency from his  
16 account at Gemini, a provider of financial services. This caused Mr. Ross  
17 significant distress because, at the time, Mr. Ross had \$500,000 in USD in his  
18 Gemini account.

19 35. At approximately the same time, Mr. Ross noticed that his AT&T  
20 mobile phone had lost service and displayed "No Service", and he also noticed that  
21 he was automatically logged out of his Gmail account.

22 36. Mr. Ross immediately suspected that a hacker attack was underway  
23 and took his mobile phone to an Apple store for assistance.

24 37. Apple representatives assisted Mr. Ross in contacting AT&T Customer  
25 Support. At that time, an AT&T employee, representative and agent informed the  
26 Apple representatives that Mr. Ross' SIM card had been changed. AT&T  
27 employees, representatives and agents advised the Apple representatives to provide  
28 Mr. Ross with a new SIM card, and then Apple employees replaced the SIM card

1 in Mr. Ross' phone. AT&T then activated the new SIM card, restoring Mr. Ross'  
2 access to his AT&T mobile number and account services.

3 38. When Mr. Ross returned home that evening, he called AT&T's  
4 customer service to discuss the unauthorized access to his account by AT&T  
5 employees, representatives and agents and the unauthorized SIM swap. An AT&T  
6 customer service representative who identified himself as Ryan S. (with a  
7 representative identification number RS410M) informed Mr. Ross that an  
8 unauthorized SIM swap had occurred on his service at approximately 5:47 PM PT  
9 by AT&T representative Cristelo V. (with a representative identification number  
10 CV921H).

11 39. AT&T representative Ryan S. also informed Mr. Ross that this  
12 unauthorized SIM swap request was made using customer owned and maintained  
13 equipment ("COAM"), and explained that COAM is a mobile phone that is not  
14 provided by AT&T and would generally be of unknown origin to AT&T (for  
15 example, a hacker might purchase a used mobile phone on the internet).  
16 Furthermore, Ryan S. expressed surprise that this SIM swap was executed as he  
17 told Mr. Ross it was against AT&T internal policies for an AT&T representative to  
18 execute a COAM-originated SIM swap request from anyone calling in to an AT&T  
19 call center. Ryan S further represented that he made a specific note of this violation  
20 of AT&T's own policy in Mr. Ross' account, reading the note verbally to Mr. Ross  
21 "I have informed customer that a SIM card and IMEI change occurred on 10/26/18  
22 at 5:47pm. This change was approved by agent which is a direct violation of the  
23 ATT activation policy." After a couple of hours on this call, Ryan S told Mr. Ross  
24 that his supervisor would take over the call, which she did, and immediately told  
25 Mr. Ross that Ryan S should not have given the information he did to Mr. Ross,  
26 and she immediately and abruptly terminated the call, causing further distress to  
27 Mr. Ross.  
28

1           40. AT&T employees, representatives and agents (including Ryan S.)  
2 represented to Mr. Ross that AT&T would place a warning on his account stating  
3 that he was experiencing fraud and instructing AT&T employees not to change  
4 anything on his account – including his SIM card.

5           41. AT&T informs its customers that verbal account passcodes—which  
6 are different than online account sign-in passwords or the passcodes used to access  
7 a mobile device—are used to protect customer’s mobile accounts and may be  
8 required when a customer manages their AT&T account online or in an AT&T  
9 store.<sup>6</sup>

10          42. Within minutes of AT&T giving control over Mr. Ross’s AT&T mobile  
11 number to the hackers, they used that control to access and take over Mr. Ross’  
12 accounts at his financial services providers, including but not limited to, Coinbase,  
13 Gemini, and Binance. Coinbase and Gemini allow their users to store US dollars  
14 that can be used to buy and sell cryptocurrencies (such as bitcoin) within the user’s  
15 account, in a similar way to how users can store US dollars used to buy and sell  
16 stocks at financial services providers such as Fidelity, Schwab, and E\*Trade.

17          43. At the time of the SIM swap attack, Mr. Ross had approximately  
18 \$500,000 in US dollars in his Gemini account and approximately \$500,000 in US  
19 dollars in his Coinbase account. By utilizing their control over Mr. Ross’ mobile  
20 phone number, which AT&T gave them, third-party hackers were able to access  
21 and take control of these accounts of Mr. Ross and control the entire USD amounts  
22 he held in both accounts. The hackers used Mr. Ross’s \$1,000,000 in US dollars to  
23 purchase bitcoin—a type of cryptocurrency that can be difficult to trace—and then  
24 the hackers transferred that bitcoin into accounts they controlled at a different  
25  
26

---

27  
28 <sup>6</sup> “Get info on passcodes for mobile accounts,” AT&T, *available at*  
<https://www.att.com/esupport/article.html#!/mobile/KM1049472?gsi=tp3wtr>.

1 financial services provider. This made the cryptocurrency exceedingly difficult to  
2 trace, let alone recover.<sup>7</sup>

3 44. The hackers also transferred cryptocurrency worth approximately  
4 \$3,000 from Mr. Ross' Binance account into accounts they controlled, thereby  
5 stealing those funds from him as well.

6 45. The hackers also used their control over Mr. Ross' AT&T mobile  
7 phone number to access, change the passwords, and take control of several of Mr.  
8 Ross' most sensitive online accounts, including, but not limited to, his Authy,  
9 Google, Yahoo!, and DropBox accounts. In taking over his Google account, the  
10 hackers also changed his passwords and the phone number linked to Mr. Ross'  
11 two-factor authentication for these accounts, which made it impossible for Mr.  
12 Ross to regain immediate access to, let alone control of, these accounts (because  
13 any requests to remind him of or reset the password no longer were sent to Mr.  
14 Ross' mobile phone, but rather to the hacker's phone). It took Mr. Ross  
15 approximately 7-10 days to regain access to and restore control over his email and,  
16 and longer for his other online personal accounts, and several weeks to regain  
17 access to the accounts taken over at his other financial services providers. In  
18 addition, the hackers deleted several weeks-worth of emails and substantial data  
19 from Mr. Ross' Google account. Mr. Ross has not been able to recover any of this  
20 data.

21 46. Criminal investigations by the California-based Regional Enforcement  
22 Allied Computer Team ("REACT"), a multi-jurisdictional law enforcement  
23 partnership specializing in cybercrime, into the October 2018 breach of Mr. Ross'  
24 AT&T account and the resulting theft revealed the involvement of a third-party

---

25 <sup>7</sup> See Investigation Report, Regional Enforcement Allied Computer Team, *California v. Nicholas*  
26 *Truglia* (Oct. 2018) (attached hereto as Exhibit B) at p. 8 ("explaining that "all of Robert R.'s  
27 funds stored in Coinbase (approximately \$500,000) and Gemini (approximately \$500,000) had  
28 been held in USD. The [hacker] used all the funds in USD at both exchanges to purchase  
bitcoins, then immediately withdrew all of the bitcoins. ... This information was subsequently  
verified by obtaining records directly from Coinbase and Gemini via search warrant.").

1 hacker named Nicholas Truglia, who was arrested by REACT detectives on  
2 November 13, 2018, and faces 21 felony counts in Santa Clara County for SIM  
3 swaps and related thefts, including against Mr. Ross. In their investigation report,  
4 REACT detectives specifically wrote that they obtained a search warrant for AT&T  
5 records pertaining to these thefts, and in response, AT&T provided REACT  
6 investigators with records that showed the same mobile device used by the hacker  
7 (identified through the device's IMEI number) had been used to effect the account  
8 takeovers of Mr. Ross, as well as the accounts of several other victims. In total, the  
9 records indicated that, prior to the unauthorized and illegal SIM swap and theft  
10 facilitated by AT&T against Mr. Ross, 11 unique phone numbers had been SIM  
11 swapped using this device between October 5 and October 26, 2018. It is  
12 incredulous that AT&T not only allowed these other unauthorized SIM swaps to  
13 happen, resulting in several other victims, but certainly knew or should have  
14 known that the same mobile device used to SIM swap other victims was already  
15 being used by a hacker who later used that same device to SIM swap Mr. Ross.  
16 Even the most basic check by AT&T would have easily flagged this IMEI as being  
17 used to perpetrate completely unauthorized and illicit SIM swaps well prior to the  
18 unauthorized and illegal SIM swap against Mr. Ross, which resulted within 45  
19 minutes of the theft of almost his entire life's savings of \$1,000,000.

20 47. Mr. Ross' financial and personal life have been uprooted as a result of  
21 AT&T's failure to safeguard his account.

22 48. As a result of the SIM swap detailed above, Mr. Ross lost more than  
23 \$1 million in USD. This money constituted the majority of Mr. Ross' life savings  
24 and the money he had saved for his daughter's college fund as well as his own  
25 retirement.

26 49. The financial strain resulting from the robbery of Mr. Ross has caused  
27 extreme emotional distress for Mr. Ross. The loss of his savings caused massive  
28 disruption in Mr. Ross' financial planning and caused him to worry about the

1 financial well-being of himself and his daughter. He has suffered, and continues to  
 2 suffer, from severe anxiety, fear, weight gain, depression, and loss of sleep as a  
 3 direct result.

4 50. Additionally, Mr. Ross' and his minor daughter's sensitive and  
 5 confidential personal information have been compromised as a result of the SIM  
 6 swaps. Mr. Ross stored color copies of their passports, drivers' licenses, and birth  
 7 certificates in the online accounts which were taken over by the hackers as a result  
 8 of the AT&T-facilitated SIM swap. Ten years of Mr. Ross' sensitive and  
 9 confidential tax returns were also compromised. All of this information is now at  
 10 extraordinarily high risk of being posted or bought and sold on the dark web by  
 11 criminals and identity thieves, putting Mr. Ross and his minor child at ongoing risk  
 12 of significant privacy violations, identity theft, and countless additional unknown  
 13 harms for the rest of their lives.

14 **C. AT&T's Failure to Protect Mr. Ross' Account from Unauthorized**  
 15 **Access Violates Federal Law**

16 51. AT&T is the world's largest telecommunications company and  
 17 provider of mobile telephone services. As a common carrier,<sup>8</sup> AT&T is governed  
 18 by the Federal Communications Act of 1934, as amended ("FCA"),<sup>9</sup> and  
 19 corresponding regulations passed by the FCC.<sup>10</sup>

20 52. Recognizing the sensitivity of data collected by mobile carriers,  
 21 Congress, through the FCA, requires AT&T to protect Mr. Ross' sensitive personal  
 22 information to which it has access as a result of its unique position as a  
 23 telecommunications carrier.<sup>11</sup>

24 53. Section 222 of the FCA, which became part of the Act in 1996,  
 25 requires AT&T to protect the privacy and security of information about its

26 <sup>8</sup> 47 U.S. Code § 153(51).

27 <sup>9</sup> 47 U.S.C. § 151 *et seq.*

28 <sup>10</sup> 47 C.F.R. § 64.2001 *et seq.*

<sup>11</sup> 47 U.S.C. § 222.



1 customers. Likewise, Section 201(b) of the Act requires AT&T's practices related  
 2 to the collection of information from its customers to be "just and reasonable" and  
 3 declares unlawful any practice that is unjust or unreasonable.<sup>12</sup>

4 54. AT&T's most specific obligations to protect its customers concerns a  
 5 specific type of information, called Customer Proprietary Information and Other  
 6 Customer Information, and known by the acronym "CPNI."<sup>13</sup> Specifically, the  
 7 FCA "requires telecommunications carriers to take specific steps to ensure that  
 8 CPNI is adequately protected from unauthorized disclosure."<sup>14</sup>

9 55. Carriers like AT&T are liable for failures to protect their customers  
 10 unauthorized disclosures.<sup>15</sup> The FCC has also stated that "[t]o the extent that a  
 11 carrier's failure to take reasonable precautions renders private customer  
 12 information unprotected or results in disclosure of individually identifiable CPNI, .  
 13 . . a violation of section 222 may have occurred."<sup>16</sup>

14 56. CPNI is defined as "information that relates to the quantity, technical  
 15 configuration, type, destination, location, and amount of use of a  
 16 telecommunications service subscribed to by any customer of a  
 17 telecommunications carrier, and that is made available to the carrier by the  
 18 customer solely by virtue of the carrier-customer relationship; and . . . information  
 19 contained in the bills pertaining to telephone exchange service or telephone toll  
 20 service received by a customer of a carrier."<sup>17</sup>

---

22 <sup>12</sup> 47 U.S.C. § 201(b).

23 <sup>13</sup> 47 U.S.C. § 222(a).

24 <sup>14</sup> Report and Order and Further Notice of Proposed Rulemaking, *In the Matter of*  
 25 *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of*  
 26 *Customer Proprietary Network Information and Other Customer Information*, 22 F.C.C. Rcd.  
 6927 ¶ 1 (April 2, 2007) (hereafter, "2007 CPNI Order").

26 <sup>15</sup> 47 U.S.C. §§ 206, 207.

27 <sup>16</sup> Declaratory Ruling, *In the Matter of Implementation of the Telecommunications Act of 1996:*  
 28 *Telecommunications Carriers' Use of Customer Proprietary Network Information & Other*  
*Customer Information*, 28 F.C.C. Rcd. 9609 ¶ 30 (2013) (hereafter, "2013 CPNI Order").

<sup>17</sup> 47 U.S.C. § 222(h)(1).



1           57. As AT&T has admitted to customers, SIM swap attacks constitute a  
2 CPNI breach.

3           58. Mr. Ross' CPNI was breached by one or more AT&T employees,  
4 representatives and agents when they accessed his account and swapped his SIM  
5 card number without his authorization. When employees, representatives and  
6 agents accessed Mr. Ross' account, his CPNI was visible. On information and  
7 belief, this included, but was not limited to, information about the configuration,  
8 type, and use of his subscribed AT&T services, his personal information, his SIM  
9 card details, and his billing information. AT&T employees, representatives and  
10 agents then used this information to effectuate an unauthorized SIM swap.

11           59. This type of unauthorized use of Mr. Ross' CPNI is illegal under the  
12 FCA. The FCA forbids AT&T from "us[ing], disclos[ing], or permit[ting] access  
13 to" CPNI, except in limited circumstances.<sup>18</sup> This extends to the carrier's  
14 employees, representatives and agents.

15           60. AT&T may only use, disclose, or permit access Mr. Ross' CPNI: (1)  
16 as required by law; (2) with his approval; or (3) in its provision of the  
17 telecommunications service from which such information is derived, or services  
18 necessary to or used in the provision of such telecommunications service.<sup>19</sup>  
19 Beyond such use, "the Commission's rules require carriers to obtain a customer's  
20 knowing consent before using or disclosing CPNI."<sup>20</sup>

21           61. AT&T failed to protect Mr. Ross from authorized use of his CPNI.  
22 AT&T permitted its employees, representatives and agents to use and/or disclose  
23 Mr. Ross' CPNI without obtaining Mr. Ross' knowing consent beforehand. AT&T  
24 employees, representatives and agents, acting within the scope of their  
25 employment and agency, likewise did not seek Mr. Ross' knowing consent before  
26

---

27 <sup>18</sup> 47 U.S.C. § 222(c)(1).

28 <sup>19</sup> 47 U.S.C. § 222.

<sup>20</sup> 2007 CPNI Order ¶ 8 (emphasis added).

1 using, disclosing, and/or permitting access to his CPNI when they accessed his  
 2 account and swapped his SIM card. Instead, AT&T employees, representatives and  
 3 agents authorized a COAM SIM swap over the phone, in violation of AT&T's own  
 4 internal policies. Because such conduct does not fit within the FCA's recognized  
 5 legitimate uses, it constitutes a violation of the FCA.

6 62. Pursuant to the FCA, the FCC has developed comprehensive rules  
 7 concerning AT&T's obligations under its duty to protect customers' CPNI.<sup>21</sup> This  
 8 includes rules "designed to ensure that telecommunications carriers establish  
 9 effective safeguards to protect against unauthorized use or disclosure of CPNI."<sup>22</sup>  
 10 The FCC specifically recognizes that "[a]bsent carriers' adoption of adequate  
 11 security safeguards, consumers' sensitive information... can be disclosed to third  
 12 parties without consumers' knowledge or consent."<sup>23</sup> In a 2013 order, the FCC  
 13 "clarif[ied] existing law so that consumers will know that *their carriers must*  
 14 *safeguard these kinds of information so long as the information is collected by or*  
 15 *at the direction of the carrier and the carrier or its designee*<sup>24</sup> *has access to or*  
 16 *control over the information.*"<sup>25</sup>

17 63. Pursuant to these rules, AT&T must "implement a system by which  
 18 the status of a customer's CPNI approval can be clearly established *prior to* the use  
 19 of CPNI."<sup>26</sup> AT&T is also required to "design their customer service records in  
 20 such a way that the status of a customer's CPNI approval can be clearly  
 21  
 22

---

23 <sup>21</sup> See 47 CFR § 64.2001("The purpose of the rules in this subpart is to implement section 222 of  
 24 the Communications Act of 1934, as amended, 47 U.S.C. 222."). The FCC also regularly  
 25 releases CPNI orders that promulgate rules implementing its express statutory obligations. See  
 2007 CPNI Order and 2013 CPNI Order.

26 <sup>22</sup> 2007 CPNI Order ¶ 9; see also *Id.* at ¶ 35; 47 U.S.C. § 222(c); 47 C.F.R. § 64.2009.

<sup>23</sup> *Id.*

<sup>24</sup> In the ruling, "designee" is defined as "an entity to which the carrier has transmitted, or  
 directed the transmission of, CPNI or is the carrier's agent." *Id.* n. 1.

<sup>25</sup> *Id.* at ¶ 1 (emphasis added).

<sup>26</sup> 2007 CPNI Order ¶¶ 8-9 (emphasis added); see also 47 C.F.R. § 64.2009(a).

1 established.”<sup>27</sup> The FCC’s rules also “require carriers to maintain records that track  
2 access to customer CPNI records.”<sup>28</sup>

3 64. Upon information and belief, AT&T has failed to implement such a  
4 system. The fact that Mr. Ross’ account was accessed, and his SIM card number  
5 was changed without his authorization, demonstrates AT&T’s failures in this  
6 regard.

7 65. AT&T is also required to “train their personnel as to when they are  
8 and are not authorized to use CPNI, and carriers must have an express disciplinary  
9 process in place.”<sup>29</sup>

10 66. Upon information and belief, AT&T has failed to properly train and  
11 supervise its personnel, contractors, representatives and agents, as reflected by an  
12 AT&T employee, representative and agent’s involvement in Mr. Ross’ breaches –  
13 and that employee, representative’s and agent’s ability to so easily effectuate a SIM  
14 swap in violation of AT&T’s own internal policies.

15 67. AT&T has also breached its duty to safeguard Mr. Ross’ CPNI from  
16 data breaches, in violation of Section 222(a) and Section 201(b) of the FCA.

17 68. The FCC has “[made] clear that carriers’ existing statutory obligations  
18 to protect their customers’ CPNI include[s] a requirement that carriers take  
19 reasonable steps, which may include encryption, to protect their CPNI databases  
20 from hackers and other unauthorized attempts by third parties to access CPNI.”<sup>30</sup>

21 69. AT&T failed to take reasonable steps to protect Mr. Ross’ CPNI,  
22 thereby allowing third-party hackers to access his CPNI.

23 70. The FCC also requires that carriers inform customers – and law  
24 enforcement – “whenever a security breach results in that customer’s CPNI being  
25

---

26 <sup>27</sup> *Id.* ¶ 9.

27 <sup>28</sup> *Id.*

28 <sup>29</sup> 47 C.F.R. § 64.2009(b) “Safeguards required for use of customer proprietary network information”.

<sup>30</sup> 2007 CPNI Order ¶ 36 (citation omitted).

1 disclosed to a third party without that customer’s authorization.”<sup>31</sup> This  
 2 requirement extends to *any* unauthorized disclosure.

3 71. In adopting this requirement, the FCC rejected the argument that it  
 4 “need not impose new rules about notice to customers of unauthorized disclosure  
 5 because competitive market conditions will protect CPNI from unauthorized  
 6 disclosure.”<sup>32</sup>

7 72. Instead, the FCC found that “[i]f customers and law enforcement  
 8 agencies are unaware of [unauthorized access], unauthorized releases of CPNI will  
 9 have little impact on carriers’ behavior, and thus provide little incentive for carriers  
 10 to prevent further unauthorized releases. By mandating the notification process  
 11 adopted here, we better empower consumers to make informed decisions about  
 12 service providers and assist law enforcement with its investigations. This notice  
 13 will also empower carriers and consumers to take whatever ‘next steps’ are  
 14 appropriate in light of the customer’s particular situation.”<sup>33</sup> The FCC specifically  
 15 recognized that this notice could allow consumers to take precautions or protect  
 16 themselves “to avoid stalking or domestic violence.”<sup>34</sup>

17 73. AT&T failed in its duty to safeguard Mr. Ross’ CPNI from breaches  
 18 and, upon information and belief, has failed to properly inform him of such  
 19 breaches when they occurred. Mr. Ross never received any documentation or  
 20 communication alerting him that his CPNI had been breached, even though AT&T  
 21 knew his CPNI had been breached as a result of the REACT criminal investigation,  
 22 and knew or should have known that his CPNI had been breached as a result of  
 23 multiple prior SIM swaps enacted by hackers using the same mobile phone and  
 24 IMEI.

26 \_\_\_\_\_  
 27 <sup>31</sup> 2007 CPNI Order at ¶ 26; *see also* 47 C.F.R. § 64.2011(c).

28 <sup>32</sup> 2007 CPNI Order ¶ 30.

<sup>33</sup> *Id.*

<sup>34</sup> *Id.* at n. 100.

1           74. Under the FCA, AT&T is not just liable for its own violations of the  
 2 Act, but also for violations that it “cause[s] or permit[s].”<sup>35</sup> By failing to secure  
 3 Mr. Ross’ account and protect his CPNI, AT&T caused and/or permitted Mr. Ross’  
 4 CPNI to be accessed and used by its own employees, representatives and agents  
 5 and by third-party hackers.

6           75. AT&T is also responsible for the acts, omissions, and/or failures of  
 7 officers, agents, employees, or any other person acting for or employed by AT&T.

8           **D. Mr. Ross’ Harm was Caused by Defendants’ Negligence**

9           76. By failing to secure Mr. Ross’ account—and protect the confidential  
 10 and sensitive data contained therein—and to properly hire, train, and supervise  
 11 their employees, representatives and agents, Defendants are responsible for the  
 12 foreseeable harm Mr. Ross suffered as a result of Defendants’ gross negligence.

13           Further, Defendants are responsible for their representatives’ and agents’  
 14 failure to obtain Mr. Ross’ valid consent before accessing his account and  
 15 effectuating a SIM swap, as such actions were within the scope of their  
 16 agency of employment with Defendants. On information and belief,  
 17 Defendants’ representatives and agents were tasked with and able to change  
 18 customers’ SIM card numbers at will – even when such changes violated  
 19 AT&T company policy. Additionally, Defendants representatives’ and  
 20 agents’ breach of Mr. Ross’ account and the subsequent SIM swap was  
 21 foreseeable. AT&T has known for more than a decade that third parties  
 22 frequently attempt to access and take over mobile customers’ accounts for  
 23 fraudulent purposes.

24  
 25  
 26 <sup>35</sup> See 47 U.S.C.A. § 206 (establishing that “[i]n case any common carrier shall do, or cause or  
 27 permit to be done, any act, matter, or thing in this chapter prohibited or declared to be unlawful,  
 28 or shall omit to do any act, matter, or thing in this chapter required to be done such common  
 carrier shall be liable to the person or persons injured thereby for the full amount of damages  
 sustained in consequence of any such violation of the provisions of this chapter[.]”)

1           77. In 2007, the FCC issued an order strengthening its CPNI rules in  
 2 response to the growing practice of “pretexting.”<sup>36</sup> Pretexting is “the practice of  
 3 pretending to be a particular customer or other authorized person in order to obtain  
 4 access to that customer’s call detail or other private communication records.”<sup>37</sup>  
 5 This 2007 Order put AT&T on notice that its customers’ accounts were vulnerable  
 6 targets of the third-parties seeking unauthorized access.

7           78. AT&T and its representatives and agents also knew, or should have  
 8 known, about the risk SIM swap crimes presented to its customers. SIM swap  
 9 crimes have been a widespread and growing problem for years. The U.S. Fair  
 10 Trade Commission (“FTC”) reported in 2016 that there were 1,038 reported SIM  
 11 swap attacks *per month* in January 2013, which increased sharply to 2,658 per  
 12 month by January 2016—2.5 times as many.<sup>38</sup> The FTC reported that SIM swaps  
 13 represented 6.3% of all identity thefts reported to the agency in January 2016, and  
 14 that such thefts “involved all four of the major mobile carriers” – including  
 15 AT&T.<sup>39</sup>

16           79. AT&T knew or should have known that it needed to take steps to  
 17 protect its customers. The FTC’s 2017 Report stated that “*mobile carriers are in a*  
 18 *better position than their customers to prevent identity theft through mobile*  
 19 *account hijacking[.]*”<sup>40</sup> The FTC urged carriers like AT&T to “adopt a multi-level  
 20 approach to authenticating both existing and new customers and require their own  
 21 employees as well as third-party retailers to use it for all transactions.”<sup>41</sup> The FTC  
 22 also specifically warned carriers like AT&T of the risk that, due to text message

---

23 <sup>36</sup> 2007 CPNI Order.

24 <sup>37</sup> *Id.* at ¶ 1.

25 <sup>38</sup> Lori Cranor, FTC Chief Technologist, “Your mobile phone account could be hijacked by an  
 26 identity thief,” Federal Trade Commission (June 7, 2016), *available at*  
 27 [https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-](https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief)  
 28 [hijacked-identity-thief](https://www.ftc.gov/news-events/blogs/techftc/2016/06/your-mobile-phone-account-could-be-hijacked-identity-thief) (hereafter, “2017 FTC Report”).

<sup>39</sup> *Id.*

<sup>40</sup> *Id.* (emphasis added).

<sup>41</sup> *Id.*

1 password reset requests and two-factor authentication, SIM swapping put  
2 subscribers at risk of financial loss and privacy violations:

3 Having a mobile phone account hijacked can waste hours of a  
4 victim's time and cause them to miss important calls and  
5 messages. However, this crime is particularly problematic due  
6 to the growing use of text messages to mobile phones as part of  
7 authentication schemes for financial services and other  
8 accounts. The security of two-factor authentication schemes  
9 that use phones as one of the factors relies on the assumption  
10 that someone who steals your password has not also stolen your  
11 phone number. *Thus, mobile carriers and third-party retailers  
need to be vigilant in their authentication practices to avoid  
putting their customers at risk of major financial loss and  
having email, social network, and other accounts  
compromised.*<sup>42</sup>

12 80. AT&T admitted it was aware of SIM swap crimes and the effect they  
13 could have on its customers in September 2017 when AT&T's Vice President of  
14 Security Platforms published an article on AT&T's "Cyber Aware" blog about SIM  
15 swaps.<sup>43</sup> In the article, AT&T acknowledged that subscribers with "valuable  
16 accounts that are accessible online" are likely targets of SIM swaps. AT&T  
17 recommended that its customers set up passcodes that would provide "extra  
18 security." These passcodes failed to protect Mr. Ross.

19 81. AT&T therefore knew that its customers' accounts were at risk for  
20 *longer than a year* before Mr. Ross' account was breached.

21 82. AT&T's inadequate security procedures are particularly egregious in  
22 light of AT&T's repeated public statements about the importance of cyber security  
23 and its public representations about its expertise in this area. AT&T has an entire  
24 series on its public YouTube channel ("AT&T ThreatTraq") dedicated to discussing  
25

26  
27 <sup>42</sup> *Id.* (emphasis added).

28 <sup>43</sup> Brian Rexroad, "Secure Your Number to Reduce SIM Swap Scams," AT&T's Cyber Aware (Sep. 2017), available at [https://about.att.com/pages/cyberaware/ni/blog/sim\\_swap](https://about.att.com/pages/cyberaware/ni/blog/sim_swap).



1 and analyzing emerging cybersecurity threats.<sup>44</sup> In its videos, AT&T describes  
 2 itself as a “network that senses and mitigates cyber threats.”<sup>45</sup>

3 83. AT&T recognizes the risks that arise when a mobile phone is  
 4 compromised, stating, “Our phones are mini-computers, and with so much  
 5 personal data on our phones today, it’s also important to secure our mobile  
 6 devices.”<sup>46</sup> AT&T’s advertisements also stress how central a role mobile phones  
 7 play in its customer’s lives, stating: “My phone is my life” and “My phone is  
 8 everything.” The same ad stresses how the inability to use a mobile phone makes  
 9 people feel “completely untethered, flailing around.”<sup>47</sup>

10 84. AT&T markets its ability to identify and neutralize emerging cyber  
 11 threats for its customers. In one video, AT&T employees discuss “threat hunting”  
 12 – which they describe as “an active threat analysis where you’re actually thinking  
 13 about your adversary.”<sup>48</sup> They claim that it’s “important” and “something [AT&T  
 14 has] been doing for a long time.”<sup>49</sup> They advise that companies should think about  
 15 “what would a hacker want to do, where would a hacker go to get my data, what  
 16 are some of the points on my network that are most vulnerable, or where is the data  
 17 flow that is potentially going to be a leakage” and state that “having threat hunting  
 18 as part of a proactive continuous program, integrating with existing security  
 19 measures, will help [you] stay ahead of the threats.”<sup>50</sup> AT&T failed to heed this  
 20 advice.

21  
 22 <sup>44</sup> “AT&T Tech Channel,” YouTube, *available at*  
<https://www.youtube.com/user/ATTTechChannel>.

23 <sup>45</sup> “AT&T – Protect Your Network with the Power of &,” VIMEO, *available at*  
<https://vimeo.com/172399153>.

24 <sup>46</sup> AT&T, “Mobile Security,” YOUTUBE (Feb. 12, 2019), *available at*  
<https://www.youtube.com/watch?v=KSPHS89VnX0>.

25 <sup>47</sup> “AT&T Mobile Movement Campaign – Ads,” VIMEO, *available at*  
<https://vimeo.com/224936108>.

26 <sup>48</sup> AT&T Tech Channel, “The Huntin’ and Phishin’ Episode,” YOUTUBE (Apr. 21, 2017),  
 27 *available at* <https://www.youtube.com/watch?v=3g9cPCiFosk>.

28 <sup>49</sup> *Id.*

<sup>50</sup> *Id.*



1           85. Not only did AT&T advise staying ahead of and addressing cyber  
2 threats, it also stressed that these practices could even help identify “insider  
3 threats”—*employees within the company or authorized representatives and agents*.

4           86. In an additional video focused on insider threats, AT&T  
5 representatives go on at length about the threat of company insiders selling  
6 corporate information *and access*, citing a survey showing that “30% [of  
7 respondents] had purposefully sent data outside of their organization at some point  
8 in time” and “14% of the people that were interviewed said they would actually  
9 sell their corporate log-ins to folks on the outside or sell that data for less than  
10 about \$250 US.”<sup>51</sup> They cited as a “significant concern” the “individuals that have  
11 privileged access, that have broad access inside an organization.”<sup>52</sup> AT&T  
12 therefore knew or should have known that there was a significant risk that its own  
13 employees, representatives and agents would provide AT&T customer data—  
14 including customer account data—and that the risk was heightened when  
15 employees had too broad of access to corporate systems, yet failed to put sufficient  
16 systems and resources in place to mitigate that risk, despite its own advice to the  
17 contrary.

18           87. AT&T has also recognized the danger presented to its customers when  
19 their email addresses are hacked, as Mr. Ross’ was as a result of AT&T’s failures.  
20 As one AT&T employee puts it: “I think most people do have something valuable  
21 [in their email accounts], which is access to all their other accounts, which you can  
22 get with a password reset.”<sup>53</sup> They call this “something worth keeping safe.”<sup>54</sup>  
23  
24

---

25 <sup>51</sup> AT&T ThreatTraq, “The Real Threat of Insider Threats,” YouTube (May 5, 2017), *available*  
26 *at* <https://www.youtube.com/watch?v=ZM5tuNiVsjs> (emphasis added).

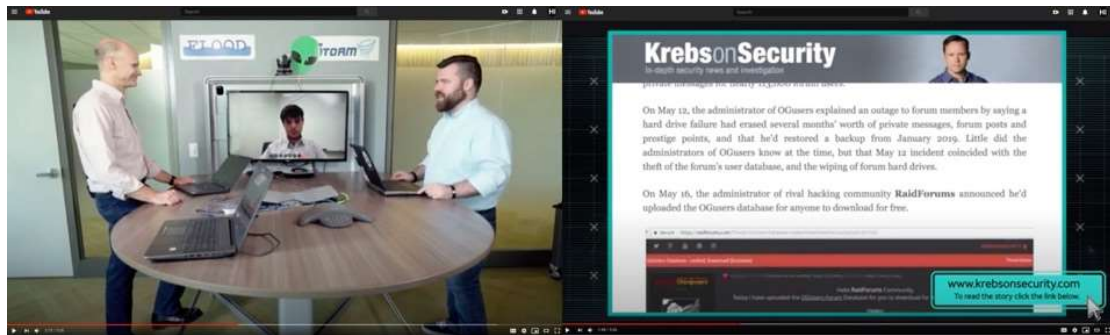
27 <sup>52</sup> *Id.*

28 <sup>53</sup> *Id.*

<sup>54</sup> *Id.* See also “Account Hijacking Forum OGusers Hacked”, KREBSONSECURITY (May 19,  
2019) *at* <https://krebsonsecurity.com/2019/05/account-hijacking-forum-ogusers-hacked/>

1 They advised that a “strong, obviously, security awareness program within a  
2 company... is extremely important.”<sup>55</sup>

3 88. In this online video series, AT&T makes specific mention of SIM  
4 swapping activity. In one video, AT&T’s Vice President of Security Platforms  
5 (Brian Rexroad) and Principal of Technology Security (Matt Keyser) discuss the  
6 hack of a forum called OGusers.<sup>56</sup> In the segment, they discuss the hacking of  
7 social media users’ account names and point to a news story that highlights—in  
8 distinct orange type—that OGusers is a forum popular among people “conducting  
9 SIM swapping attacks to seize control over victims’ phone numbers.”<sup>57</sup>



16 Figure 1

17 AT&T’s Vice President of Security Platforms (Brian Rexroad) and Principal of  
18 Technology Security (Matt Keyser) discuss the hack of the “OGusers” forum where Sim  
19 swappers meet and a news story highlighting how SIM swappers seize control of victims’  
20 phone numbers.

21 89. AT&T was therefore well aware of the significant risk that AT&T  
22 employees, representatives and agents and SIM swapping presented to its  
23 customers, and the need to mitigate such risks, but nonetheless failed to take  
24 adequate steps to protect Mr. Ross. Instead, it continued to make public statements

25 <sup>55</sup> *Id.*

26 <sup>56</sup> AT&T ThreatTraq, “5/31/19 Account-hacking Forum OGusers Hacked,” YOUTUBE (May 31  
27 2019), available at [https://www.youtube.com/watch?time\\_continue=234&v=cS4xV3cej3A](https://www.youtube.com/watch?time_continue=234&v=cS4xV3cej3A).

28 <sup>57</sup> *Id.*; see also Freeman Indictment at ¶ 2 (Describing how “discussions—such as discussing the  
manner and means to [SIM swap] attacks generally, and networking among [SIM swap  
hackers]—typically took place on forums such as “OGusers.”).

1 giving rise to a reasonable expectation that AT&T could—and would—protect its  
2 customers.

3 90. That Mr. Ross was at risk of account breaches at the hands of AT&T  
4 employees, representatives and agents is particularly foreseeable—and AT&T’s  
5 failures are particularly stark—in light of AT&T’s history of unauthorized  
6 employee, representative and agent access to customer accounts.

7 91. In 2015, AT&T became subject to an FCC enforcement action, and  
8 paid a \$25 million civil penalty, for nearly identical failures to protect its  
9 customers’ sensitive account data.<sup>58</sup> In that case, as AT&T admitted, employees,  
10 representatives and agents at an AT&T call center breached 280,000 customers’  
11 accounts.<sup>59</sup> Specifically, AT&T employees, representatives and agents had  
12 improperly used login credentials to access customer accounts and access customer  
13 information that could be used to unlock the customers’ devices.<sup>60</sup> The employees  
14 then sold the information they obtained from the breaches to a third party.<sup>61</sup>

15 92. The FCC concluded that AT&T’s “failure to reasonably secure  
16 customers’ proprietary information violates a carrier’s statutory duty under the  
17 Communications Act to protect that information, and also constitutes an unjust and  
18 unreasonable practice in violation of the Act.”<sup>62</sup>

19 93. The FCC stressed that the FCA is intended to “ensure that consumers  
20 can trust that carriers have taken appropriate steps to ensure that unauthorized  
21 persons are not accessing, viewing or misusing their personal information.”<sup>63</sup> It  
22  
23

24  
25 <sup>58</sup> *In the Matter of AT&T Servs., Inc.*, 30 F.C.C. Rcd. 2808 (2015) at  
<https://docs.fcc.gov/public/attachments/DA-15-399A1.pdf>

26 <sup>59</sup> *Id.* at ¶ 1.

27 <sup>60</sup> *Id.* at ¶¶ 7, 11.

28 <sup>61</sup> *Id.* at ¶ 1.

<sup>62</sup> *Id.* at ¶ 2.

<sup>63</sup> *Id.*

1 stressed its expectation that “telecommunications carriers such as AT&T... take  
2 ‘every reasonable precaution’ to protect their customers’ data[.]”<sup>64</sup>

3 94. As part of its penalty, AT&T entered into a stipulated Consent Decree  
4 with the FCC, in which AT&T agreed to develop and implement a compliance plan  
5 to ensure appropriate safeguards to protect consumers against similar breaches by  
6 improving its privacy and data security practices.<sup>65</sup>

7 95. This FCC enforcement action underscores AT&T’s knowledge of the  
8 risk its employees presented to customers, the prevalence of employee breaches to  
9 customer data, the sensitive nature of customer CPNI, and its duties to protect and  
10 safeguard that data. Nonetheless, more than 3 years after stipulating to the Consent  
11 Decree, AT&T still failed to protect its customer from employee breaches of  
12 customer CPNI and other account data, virtually identical to the breach at issue  
13 here, heightening the degree of its negligence.

14 96. In January 2020, Princeton researchers released a study finding that  
15 top U.S. mobile carriers, including AT&T, do little to protect customers from SIM  
16 swap fraud.<sup>66</sup> The study stated “We examined the authentication procedures used  
17 by five prepaid wireless carriers when a customer attempted to change their SIM  
18 card. ***We found that all five carriers used insecure authentication challenges***  
19 ***that could be easily subverted by attackers.*** We also found that attackers generally  
20 only needed to target the most vulnerable authentication challenges, because the  
21 rest could be bypassed.” The researchers pretended to be the true phone owner and  
22 said they forgot answers to security questions study stating, “Our key finding is  
23 that, at the time of our data collection, all 5 carriers used insecure authentication  
24 challenges that could easily be subverted by attackers.” The study also found: (i)

25 <sup>64</sup> *Id.*

26 <sup>65</sup> *Id.* at ¶¶ 2, 17-18, 21.

27 <sup>66</sup> “*An Empirical Study of Wireless Carrier Authentication for SIM Swaps*” Kevin Lee, Ben  
28 Kaiser, Jonathan Mayer, Arvind Narayanan Dept of Computer Science and Center for  
Information Technology Policy, Princeton University, January 10, 2020 at  
[https://www.issms2fasecure.com/assets/sim\\_swaps-01-10-2020.pdf](https://www.issms2fasecure.com/assets/sim_swaps-01-10-2020.pdf)

1 Callers only needed to successfully respond to one challenge in order to  
 2 authenticate, even if they had failed numerous prior challenges. (ii) Four-fifths of  
 3 SIM-swap fraud attempts were successful, and the researchers attempted 50 SIM  
 4 swaps and successfully completed 39. (iii) AT&T, Verizon and T-Mobile failed the  
 5 study. (iv) Some carriers even guided them to the correct answer or didn't ask for  
 6 anything at all. The Princeton study was widely reported in the media and  
 7 prompted Congress to get involved. In January 2020, Senator Ron Wyden and 5  
 8 other Senators and Congressmen published a letter to FCC Chairman Ajit Pai  
 9 calling on him to take action to protect consumers against SIM swap fraud, with  
 10 the Senator stating "SIM swap fraud may also endanger national security. For  
 11 example, if a cybercriminal or foreign government uses a SIM swap to hack into  
 12 the email account of a local public safety official, they could then leverage that  
 13 access to issue emergency alerts using the federal alert and warning system  
 14 operated by the Federal Emergency Management Agency."<sup>67</sup> Senator Wyden also  
 15 stated, "Consumers are at the mercy of wireless carriers when it comes to being  
 16 protected against SIM swaps."<sup>68</sup>

17 97. According to a Wall Street Journal ("WSJ") article from November  
 18 2019, "He Thought His Phone Was Secure; Then He Lost \$24 Million to Hackers,"  
 19 investigators say they know of more than 3,000 SIM swap victims, accounting for  
 20 at least \$70 million in theft nationwide (the real numbers are likely much higher  
 21 considering that many cases go unreported).<sup>69</sup> The WSJ article states, "the people  
 22 who investigate these attacks consider them some of the most harmful they have  
 23 ever seen." <sup>69</sup> Victims include high profile public officials, celebrities, and business  
 24 executives like Jack Dorsey, the CEO of Twitter, whose 2019 SIM swap hack was  
 25 profiled in the Forbes article "Why Twitter Blames AT&T For The Hack Of Its  
 26

<sup>67</sup> <https://docs.fcc.gov/public/attachments/DOC-362599A1.pdf>

<sup>68</sup> <https://twitter.com/ronwyden/status/1215757690875600896>

<sup>69</sup> <https://www.wsj.com/articles/he-thought-his-phone-was-secure-then-he-lost-24-million-to-hackers-11573221600>.

1 CEO Jack Dorsey Account, Sending Shocking Racist Tweets,” and quotes Jeb Su,  
 2 a Principal Analyst at Atherton Research as saying “*AT&T’s poor security policy*  
 3 *made this malicious [SIM swap] hack possible.*”<sup>70</sup> The same hacker who executed  
 4 Jack Dorsey’s SIM swap also successfully hacked the District Attorney  
 5 prosecuting the hacker who AT&T gave control to Mr. Ross’ phone service.<sup>71</sup>

6 98. The SIM swap problem is exacerbated by AT&T’s sprawling,  
 7 mismanaged and problematic call center system. In 2017, AT&T’s parent (AT&T,  
 8 Inc.) had 254,000 employees<sup>72</sup> and 38 third-party call centers across eight non-US  
 9 countries.<sup>73</sup> A study by the Communication Workers of America (“CWA”) entitled  
 10 “AT&T 2018 Jobs Report: Telecom Giant Hollows Out Middle Class Workforce  
 11 and Outsources to Global Contractors, Even as it Reaps Tax Windfall” details how  
 12 AT&T’s call center operation is fundamentally broken. Among the key findings  
 13 were that (i) employees at AT&T vendor call centers face inadequate training and  
 14 intense pressure to reach unrealistic quotas – making it difficult to meet  
 15 customer’s needs; (ii) overseas vendors, paid as little as \$1.60 per hour and often  
 16 rely on other members of their household to make ends meet, provide inaccurate  
 17 information, fail to solve problems, offer credits or promotions that cannot be  
 18 honored, and enroll customers in services they did not request; and (iii) the  
 19 problems caused by overseas operations add to the burden of U.S. based workers,  
 20 thereby affecting their work. On information and belief, all of AT&T’s numerous  
 21 customer service representatives are authorized to perform SIM swaps,  
 22 exacerbating the problem. In order to address its organizational failings, AT&T

23  
 24 <sup>70</sup> <https://www.forbes.com/sites/jeanbaptiste/2019/08/31/why-twitter-blames-att-for-ceo-jack-dorsey-account-hack-sending-shocking-racist-tweets/>.

25 <sup>71</sup> “Authorities Arrest Alleged Member of Group That Hacked Jack Dorsey”, Vice by Joseph  
 26 Cox, November 23, 2019 at [https://www.vice.com/en\\_us/article/gyzawx/authorities-arrest-](https://www.vice.com/en_us/article/gyzawx/authorities-arrest-suspected-jack-dorsey-hacker)  
[suspected-jack-dorsey-hacker](https://www.vice.com/en_us/article/gyzawx/authorities-arrest-suspected-jack-dorsey-hacker).

27 <sup>72</sup> <https://www.statista.com/statistics/220683/number-of-atundt-employees-since-2007/>

28 <sup>73</sup> New Report Pulls Back the Curtain on AT&T’s Vast Network of Offshored Call Centers at  
[https://cwa-union.org/news/releases/new-report-pulls-back-curtain-on-atts-vast-network-of-](https://cwa-union.org/news/releases/new-report-pulls-back-curtain-on-atts-vast-network-of-offshored-call-centers)  
[offshored-call-centers](https://cwa-union.org/news/releases/new-report-pulls-back-curtain-on-atts-vast-network-of-offshored-call-centers)



1 could have created a call center dedicated to SIM swaps, and properly vetted,  
2 trained and supervised SIM swap customer service representatives, in order to  
3 address the problem of unauthorized SIM swaps.

4 99. Further compounding AT&T's problem-ridden call center and SIM  
5 swap mess is how AT&T apparently implemented completely inconsistent  
6 authentication protocols at their wholly-owned call centers as compared to their  
7 third-party call centers (such as One Touch Direct). An AT&T employee named  
8 Robin told Mr. Ross on August 19, 2020 (when Mr. Ross called in via AT&T's  
9 "611" feature from his phone, which apparently is routed to an AT&T wholly  
10 owned call center) that at the time of the fraudulent SIM swap executed against  
11 him (at the AT&T third-party call center One Touch Direct), callers requesting a  
12 SIM swap to a customer service representative at an AT&T wholly-owned call  
13 center received a text confirmation code that the caller needed to provide to the  
14 AT&T customer service representative to complete the SIM swap, whereas  
15 customers routed to an AT&T third-party call centers (such as One Touch Direct)  
16 did not have receive such a text confirmation, and this was because AT&T did not  
17 deploy this simple security confirmation solution to callers routed to AT&T third-  
18 party call centers. Indeed, the AT&T employee Robin confirmed to Mr. Ross that  
19 on the date of the unauthorized SIM swap, AT&T did ***not*** send a text confirmation  
20 to Mr. Ross and Robin also told Mr. Ross that the AT&T representative Ryan S  
21 made a note of that in Mr. Ross' customer record on the day of the unauthorized  
22 SIM swap.

23 100. More significantly, for many years AT&T has been fully aware of  
24 well-established technology solutions to deter and prevent unauthorized SIM  
25 swaps and resulting thefts, which it could easily have implemented well *before* Mr.  
26 Ross' phone was SIM swapped, but failed and refused to implement:

27 a. Location detection. At the exact moment of the SIM swap  
28 request, AT&T knew the hacker's phone was in New York City (as detailed in the

location data AT&T provided to REACT)<sup>74</sup> and that Mr. Ross' phone was simultaneously in San Francisco, as AT&T tracks customers' location and even sells their location data.<sup>74</sup> AT&T knew that Mr. Ross and his phone could not simultaneously be in both San Francisco and New York City, and could have easily recognized the SIM swap request as a fraud attempt, denied it, and alerted Mr. Ross. AT&T was actually profiting off customers' location data at the same time as it did nothing to use the same location data to prevent the unauthorized SIM swap.

b. Text message. AT&T could have simply sent Mr. Ross a text message asking him to confirm whether he requested the SIM swap. He would have replied "no" and AT&T would have then denied the hacker's SIM swap request and could have reported the fraud attempt to Mr. Ross. Banks regularly text customers in this way to confirm even small, low-risk transactions to prevent fraud, as in the text Mr. Ross received from Bank of America confirming \$1 transactions in Figure 2.

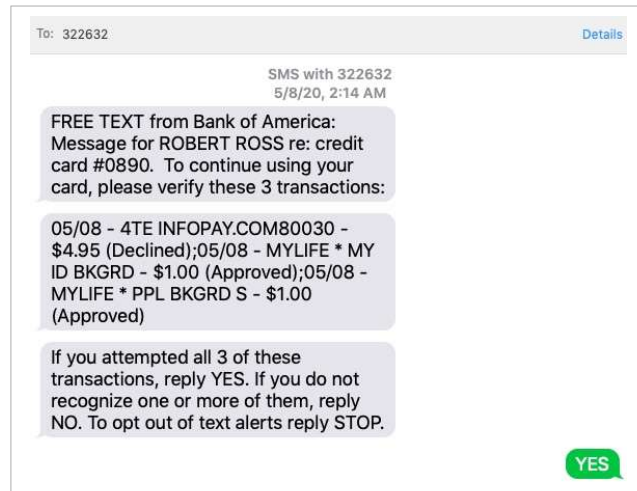


Figure 2

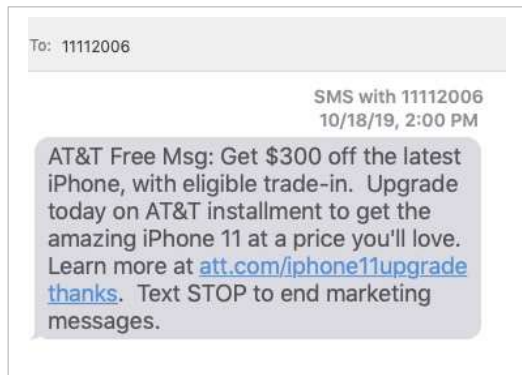
A text message from Bank of America to Mr. Ross asking him to confirm

<sup>74</sup> FCC Proposes Over \$200 Million in Fines Against Four Largest Wireless Carriers For Apparently Failing to Adequately Protect Consumer Location Data February 28, 2020 at <https://docs.fcc.gov/public/attachments/DOC-362754A1.pdf>



1 \$1 transactions, for the purpose of preventing even low-risk transactions.

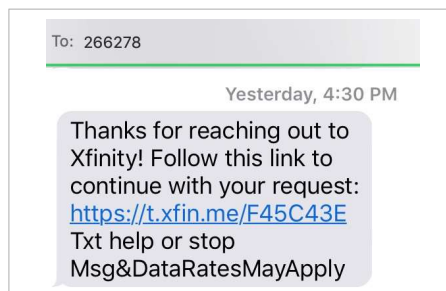
2 AT&T regularly sends text messages to its customers for marketing purposes, and  
3 asks customers to reply if they want to stop receiving such texts, as in the message  
4 AT&T sent to Mr. Ross in Figure 3.  
5



12 Figure 3

13 A text message from AT&T to Mr. Ross promoting \$300 off the latest iPhone in  
14 exchange for an installment upgrade to AT&T's service.

15 AT&T obviously has the ability to send such simple text messages to its customers  
16 requesting a reply. As a direct result of the theft of his life savings due to the SIM  
17 swap facilitated by AT&T, Mr. Ross eventually had to cancel his Comcast Xfinity  
18 cable TV service, as he could no longer afford it. During Mr. Ross' call with  
19 Comcast to request the cancellation, Comcast sent a text confirmation with a web  
20 link that required him to reconfirm the request as displayed in Figure 4.



26 Figure 4

27 Text from Comcast confirming Mr. Ross' request to cancel his service  
28

Comcast is a direct competitor to AT&T Mobility, as Comcast launched its wireless service branded as Xfinity Mobile, using Verizon's network in 2017<sup>75</sup>. With every text confirmation Mr. Ross now receives such as from Bank of America, Comcast and others, he re-lives and is reminded of the theft as it would have been so easy for AT&T to have avoided destroying his life, with a simple text message.,

c. Email confirmation. AT&T could have simply sent Mr. Ross an email asking him to confirm whether he requested the SIM swap. AT&T could have asked for a confirmation directly within the email or directed him to a legitimate link to confirm the request. Mr. Ross would have replied "no" and AT&T would have then denied the hacker's SIM swap request and could have reported the fraud attempt to Mr. Ross.

d. IMEI detection. AT&T detects when the same phone has been used in prior unauthorized SIM swaps, and their records (as provided to REACT) show that, prior to the unauthorized SIM swap AT&T facilitated against Mr. Ross, the same device as identified by its IMEI was used in 11 previous unauthorized SIM swaps.<sup>7</sup> AT&T could simply have denied the ability for the phone that was used in previous unauthorized SIM swaps to be used in subsequent SIM swaps, including Mr. Ross', and also could have alerted Mr. Ross to the fraud attempt.

e. Voice biometrics. Voice biometrics (or "Voice Id") is a well-established and cost-effective technology that has been implemented by leading financial institutions (e.g., Chase, Wells Fargo and Schwab) to prevent fraud by verifying customers' identities by comparing a caller's voice to a customer (or fraudster) voiceprint stored on file.<sup>76</sup> The technology has also been implemented by

<sup>75</sup> Xfinity Mobile at <https://corporate.comcast.com/company/xfinity/mobile> and <https://corporate.comcast.com/company/xfinity/mobile>

<sup>76</sup> Chase at <https://www.chase.com/personal/voice-biometrics>, Wells Fargo at <https://www.wellsfargo.com/privacy-security/voice-verification>, and Schwab at <https://www.schwab.com/voice-id>.

1 in Europe, including by the largest carrier in Europe, Deutsche Telekom.<sup>77</sup> While  
 2 AT&T developed its own voice biometrics solution called AT&T Watson, the  
 3 technology was never implemented to prevent SIM swaps, and instead was sold to  
 4 Interactions Corporation (“Interactions”) in 2014 in exchange for an equity stake.<sup>78</sup>  
 5 Ironically, Interactions continues to promote its voice biometrics solution as “Secure  
 6 and Convenient Authentication,”<sup>79</sup> continues to publicly promote the solution to its  
 7 large corporate customers who have their own call centers (e.g., banks, insurance  
 8 companies), publishing a research report entitled “4 emerging technologies that  
 9 could transform your contact center,” which provides in relevant part as  
 10 follows: Even as companies take steps to guard their IT environments against a  
 11 growing barrage of cyberthreats, many are neglecting another vulnerable area: their  
 12 contact centers.

13  
 14 Social engineering calls to contact centers — in which  
 15 fraudsters pose as customers and try to trick agents into  
 16 revealing confidential customer information — are on the  
 17 rise, according to industry experts, particularly at  
 financial institutions, insurance companies and other  
 businesses that store sensitive data.

18 Voice biometrics can help your agents know exactly with  
 19 whom they’re talking when they answer a customer call.  
 20 This technology can recognize voice characteristics  
 21 passively and verify callers in real time, whether they  
 22 need to speak to one of your representatives or are using  
 your interactive voice response system.

23 “By comparing your callers’ voiceprints against a  
 24 database of known fraudster voiceprints, voice biometrics

25 <sup>77</sup> *Deutsche Telekom turns to biometrics for authentication and fraud detection*

26 <https://telecoms.com/491915/dt-turns-to-biometrics-for-authentication-and-fraud-detection/>

27 <sup>78</sup> *AT&T and Interactions Agree to Strategic Transaction in Speech and Multi-Modal Technology*  
 28 *Arena* November 5, 2014.

[https://about.att.com/story/att\\_and\\_interactions\\_agree\\_to\\_strategic\\_transaction\\_in\\_speech\\_and\\_multi\\_modal\\_technology\\_arena.html](https://about.att.com/story/att_and_interactions_agree_to_strategic_transaction_in_speech_and_multi_modal_technology_arena.html)

<sup>79</sup> <https://www.interactions.com/products/voice-biometrics/>

1 programs can help you identify and track potential  
2 thieves before they steal your data.”<sup>80</sup>

3 f. Data sharing. Mobile phone carriers in other countries have  
4 implemented a “data sharing” solution to prevent theft once an unauthorized SIM  
5 swap has occurred. In essence, the carriers allow financial institutions real-time  
6 access to their SIM swap data so that the institution can block a requested currency  
7 transfer if there has been a SIM swap within a specified time frame (e.g., within 48  
8 hours of the transfer request), since very recent SIM swap combined with a  
9 withdrawal request is a strong indicator of fraud. The data sharing solution is  
10 widely known and broadly used by major carriers outside of the US. Wired  
11 magazine published an article entitled “The SIM Swap Fix That the US isn’t  
12 Using,” which states in relevant part that “While foreign phone carriers are sharing  
13 data to stop SIM swap fraud, US carriers are dragging feet.”<sup>81</sup> Wired describes that  
14 even carriers in developing countries such as Mozambique implemented the  
15 solution within a few months of understanding the extent of the problem, and that  
16 the Head of IT, Cyber Security & Core Data Networks at Vodacom reported that  
17 “[the solution] reduced their SIM swap fraud to nearly zero overnight”.<sup>82</sup> Third  
18 party aggregators such as Prove.com (formerly Payfone, Inc.) and TeleSign  
19 Corporation, who license SIM swap data from non-US carriers and sell it as a fraud  
20 prevention offering to banks. Figure 5 shows how all four major carriers in the  
21 United Kingdom (“UK”), including British Telecom, Vodafone, O2 and Three,  
22 provide their SIM swap data to Prove.com, which in turn sells a fraud prevention  
23

24  
25 <sup>80</sup> “4 Emerging Technologies That Could Transform Your Contact Center” Mike Rajich, AT&T  
26 Director of Contact Center and Enterprise Routing Product Management, AT&T  
27 <https://www.business.att.com/learn/research-reports/4-emerging-technologies-that-could-transform-your-contact-center.html>

28 <sup>81</sup> *The SIM Swap Fix That the US Isn’t Using*, Wired, Andy Greenberg, April 26, 2019  
<https://www.wired.com/story/sim-swap-fix-carriers-banks/>.

<sup>82</sup> Id.

service to banks enabling them to do real-time SIM swap checks to at the time of customers' high-risk transactions.<sup>83</sup>

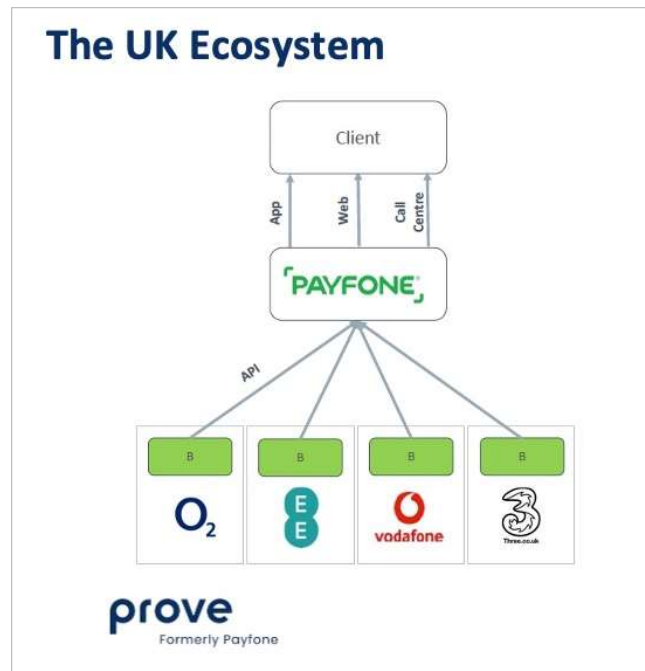


Figure 5

Prove.com system for aggregating SIM swap data from the top 4 UK carriers and enabling clients, such as banks, to perform real-time SIM swap checks

101. Had AT&T implemented any of the foregoing low cost and easy to implement technology solutions, Mr. Ross would not have been the victim of an unauthorized SIM swap.

102. Instead of implementing solutions to *prevent* unauthorized SIM swaps, AT&T appears to have made the conscious business decision to profit from unauthorized SIM swaps *after* they have occurred. On September 18, 2018, six weeks before Mr. Ross' SIM swap, AT&T, Verizon and T Mobile publicly

<sup>83</sup> <https://info.prove.com/psd2-sca-uk-mobile-authentication>

announced the joint business scheme they had been developing for months called “Project Verify,” now known as ZenKey, to profit from the SIM swap problem.<sup>84</sup>

103. ZenKey is marketed to consumers as an easier and more secure way to log into other online services, stating “Your carrier has a unique ability to identify and protect your mobile identity” and that ZenKey checks for suspicious activity at the carrier (Figure 6), denoting a real-time SIM swap check (as this is the most significant suspicious activity that can occur in a customer’s mobile account).<sup>85</sup>

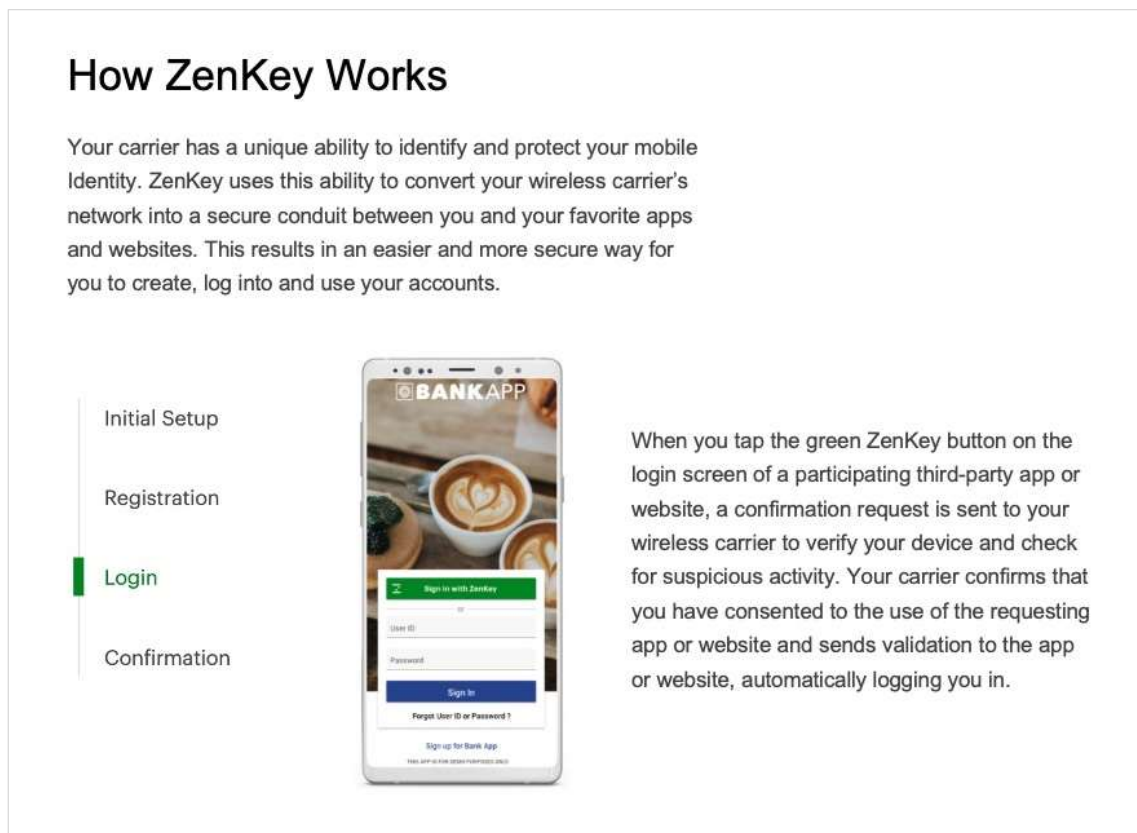


Figure 6

AT&T/ZenKey promotes that it “has a unique ability to identify and protect your mobile identity” and checks for suspicious activity.

<sup>84</sup> *U.S. Mobile Giants Want to be Your Online Identity* at

<https://krebsonsecurity.com/tag/project-verify/>

<sup>85</sup> <https://myzenkey.com/how-it-works/>

AT&T's ZenKey consumer app is available to consumers currently in the Apple and Google app stores for iPhone and Android devices, as shown in Figure 7.<sup>86</sup>

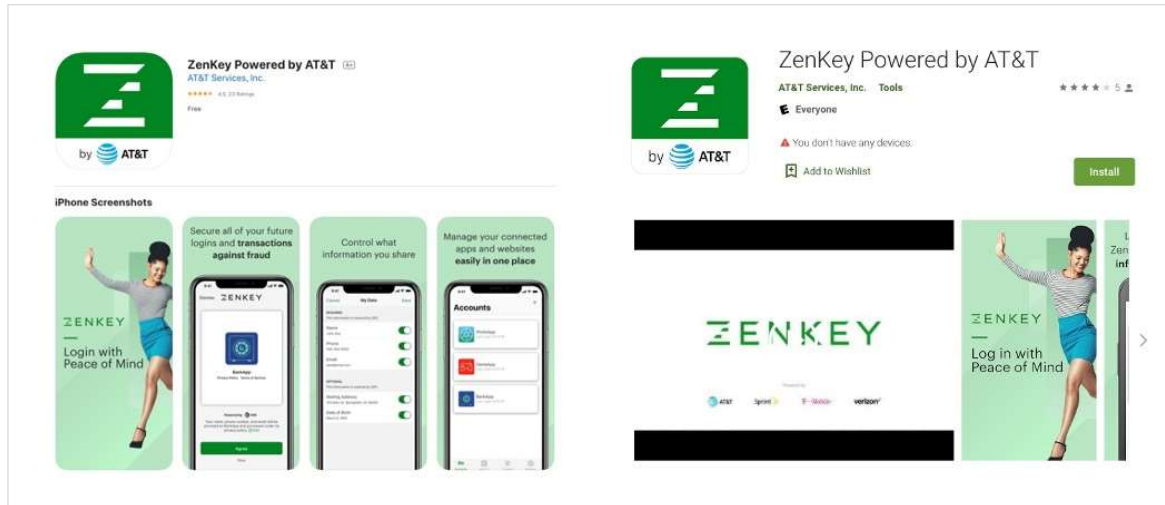


Figure 7

AT&T ZenKey apps for iPhone and Android

At the same time, ZenKey is marketed to financial institutions as an identity and authentication scheme through its “Trust Services” offering, to prevent fraud, with the clear representation that its purpose is to combat SIM swap fraud: “SIM Swap Fraud has already cost businesses hundreds of millions of dollars and the threat is increasing. With ZenKey, fraudsters can no longer access your users’ accounts based on stolen credentials and a simple SIM Swap.”<sup>87</sup> ZenKey’s benefits page states “SIM swap fraud is on the rise and has cost businesses hundreds of millions of dollars ZenKey offers a suite of APIs and event alerts (Trust Services) for Service Providers to receive on-demand fraud signals and automatic indicators.”<sup>88</sup> The ZenKey Trust Services proposal, as shown in Figure 8 is effectively executing the same type of real-time SIM swap database check as the data sharing method as described above.

<sup>86</sup> iPhone app at <https://apps.apple.com/us/app/zenkey-powered-by-at-t/id1490293601>, Android app at [https://play.google.com/store/apps/details?id=com.att.cso.consumer.MKapp&hl=en\\_US](https://play.google.com/store/apps/details?id=com.att.cso.consumer.MKapp&hl=en_US)

<sup>87</sup> <https://myzenkey.com/trust-services/>

<sup>88</sup> <https://myzenkey.com/business-benefits/>



**Trust Services**

ZenKey Trust Services are a collection of various APIs and Event Alerts that will be useful when businesses suspect fraud with user accounts.

**Get Protection from SIM Swap Fraud**

SIM Swap Fraud has already cost businesses hundreds of millions of dollars and the threat is increasing.

With ZenKey, fraudsters can no longer access your users' accounts based on stolen credentials and a simple SIM Swap. Instead, ZenKey requires new SIM cards and devices go through a robust recovery process that the user has setup beforehand.

In addition to these built-in fraud prevention features, ZenKey also offers you two other options that identify when a users' SIM changes – one via API and one via an automatic event alert that you can subscribe to.

**SIM Tenure API**

We are pleased to announce limited availability under our trial agreement for our first Trust Service – SIM Tenure API. This API gives you the ability to query for and obtain information about SIM Tenure for your users. Register now for more information.

[Register for Trust Services](#)




Figure 8

ZenKey's "Trust Services" offering for financial institutions

ZenKey seeks to charge fees to financial institutions in exchange for doing real-time checks against carrier databases to verify when a SIM swap (authorized or not) was last done,<sup>89</sup> and its Portal Agreement Terms of Service provides that "Certain services accessed or available through the [ZenKey] Portal, especially services for which You [e.g. a bank] are asked to subscribe or pay money, may have their own terms and conditions, including but not limited to the Service

<sup>89</sup> ZenKey website at <https://myzenkey.com/trust-services/>



1 Agreement.”<sup>90</sup> *ZenKey has failed to date in the marketplace, and has not yet been*  
 2 *adopted by financial institutions.*

3 104. By not implementing even basic solutions to mitigate, let alone  
 4 substantially reduce SIM swap fraud, AT&T maintains a larger revenue opportunity  
 5 for ZenKey, as more unauthorized SIM swaps lead to more fraud at banks, which  
 6 result in a greater need for banks to pay for and check SIM swap data in real-time.  
 7 While ZenKey has failed to date in the marketplace, and has not yet been adopted  
 8 by financial institutions, AT&T and its ZenKey partner-competitors continue to  
 9 invest in it (to date, they have invested around \$200 million), promote it and  
 10 develop it, rather than implement simple solutions to broadly prevent unauthorized  
 11 SIM swaps.

12 105. Rather than having easily and expeditiously implemented a data  
 13 sharing solution in which AT&T licensed their SIM swap database to third party  
 14 aggregators (such as Prove.com<sup>91</sup> or TeleSign Corporation<sup>92</sup>) or directly to financial  
 15 institutions (such as Coinbase or Gemini), to enable them to do real-time database  
 16 checks at the time of a high-risk transactions (as non-US carriers do<sup>81</sup>), AT&T  
 17 focused its efforts developing ZenKey in collusion with Verizon and T-Mobile in  
 18 their ill-conceived (and to-date failed) attempt to more directly profit and control  
 19 the authentication market opportunity.

20 **F. Defendants Are Liable for the Acts of Their Employees,**  
 21 **Representatives and Agents**

22 106. Defendants are liable for the acts of their employees, representatives  
 23 and agents who facilitated the unauthorized access to, and resulting theft from, Mr.  
 24 Ross.

25 <sup>90</sup> <https://portal.myzenkey.com/terms>

26 <sup>91</sup> *The End of Dangerous SIM Swap Fraud is Here: Payfone Extends Real-Time SIM Swap*  
 27 *Detection Algorithms* at [https://www.payfone.com/press/the-end-of-dangerous-sim-swap-fraud-](https://www.payfone.com/press/the-end-of-dangerous-sim-swap-fraud-is-here/)  
 28 [is-here/](https://www.payfone.com/press/the-end-of-dangerous-sim-swap-fraud-is-here/)

<sup>92</sup> How TeleSign Protects Transactions from SIM Swap Fraud at  
<https://www.telesign.com/blog/how-tesesign-protects-transactions-from-sim-swap-fraud>

1           107. Defendants failed to put in place adequate systems and procedures to  
2 prevent the unauthorized employee, representative and agent access to Mr. Ross’  
3 account and related data. Defendants failed to properly hire and supervise their  
4 employees, representatives and agents, allowing them to access Mr. Ross’ sensitive  
5 and confidential account data without his authorization and provide that data to  
6 third parties.

7           108. In the context of AT&T’s enterprise as a telecommunications carrier,  
8 an employee, representative and agent accessing a customer’s account information  
9 and effectuating a SIM swap—even without authorization—is not so unusual or  
10 startling that it would be unfair to include the loss resulting from such unauthorized  
11 access among other costs of AT&T’s business – particularly in light of AT&T’s  
12 awareness of the risk of SIM swaps to its customers.

13           109. Further, imposing significant liability on AT&T and its agents may  
14 prevent recurrence of SIM swap behavior because it creates a strong incentive for  
15 vigilance and proper safeguarding of customers’ data by AT&T—which, in the case  
16 of its customers, is the sole party in the position to guard substantially against this  
17 activity, as it is the custodian and guardian of this data.

18           110. As a customer of AT&T, Mr. Ross is entitled to rely upon the  
19 presumption that AT&T and the employees, representative and agents entrusted  
20 with the performance of AT&T’s business have faithfully and honestly discharged  
21 the duty owed to him by AT&T, and that they would not gain unauthorized access to  
22 his account.

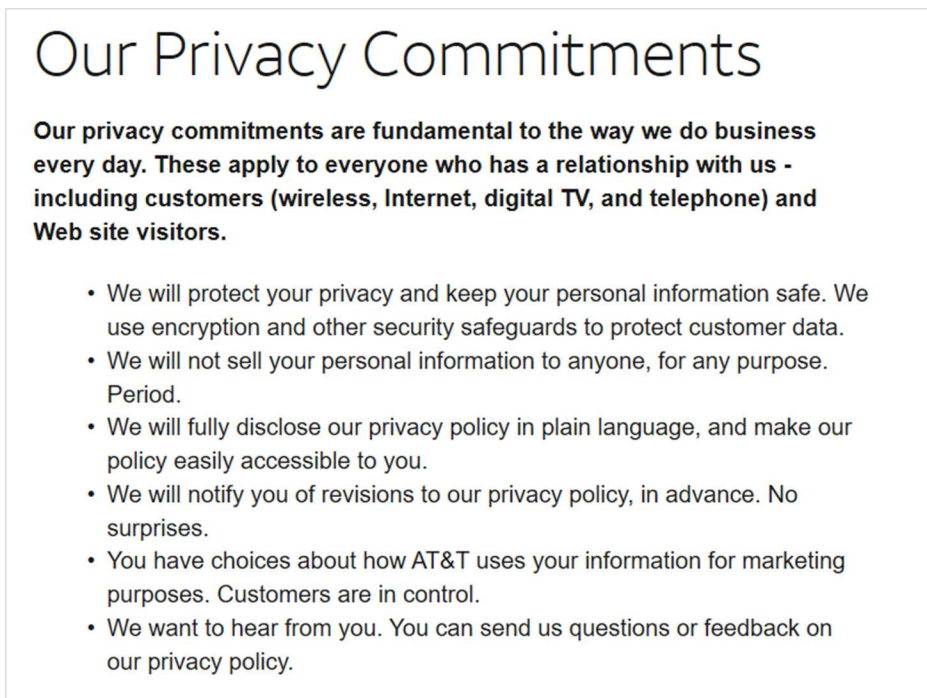
23           111. The reasonableness of Mr. Ross’ expectations that AT&T would  
24 safeguard his data is confirmed by the fact that the federal agency responsible for  
25 overseeing AT&T’s duties to its customers, the FCC, has stated that it “fully  
26  
27  
28

1 expect[s] carriers to take every reasonable precaution to protect the confidentiality  
2 of proprietary or personal customer information.”<sup>93</sup>

### 3 **AT&T’s Misrepresentations and Omissions.**

4 112. AT&T’s Privacy Policy, and the “Privacy Commitments” included  
5 therein, falsely represents and fails to disclose material information about its data  
6 security practices.

7 113. In its Privacy Policy, AT&T promised to protect Mr. Ross’ privacy and  
8 personal information, including by using “security safeguards.” AT&T further  
9 pledges that it will not sell customer data. These representations created an  
10 expectation that Mr. Ross’ AT&T account and associated data would be safe and  
11 secure, that employees, representatives and agents would not access his account  
12 without authorization, that his data would be protected from unauthorized  
13 disclosure, and that he could control how and when his data was accessed. Figure 9,  
14 immediately below, is an excerpt from AT&T’s Privacy Policy.



26 Figure 9 <sup>94</sup>

27 <sup>93</sup> 2007 CPNI Order ¶ 64.

28 <sup>94</sup> “Privacy Policy,” AT&T, attached hereto as Exhibit C.

1           114. AT&T's representation that it "uses encryption and other security  
2 safeguards to protect customer data" is false and extremely misleading.

3           115. As alleged fully above, AT&T allowed its employees, representatives  
4 and agents to access Mr. Ross' account, and the CPNI and other sensitive data  
5 contained therein, without his authorization. AT&T's statement that it would use  
6 encryption and other security safeguards to protect customers' data is therefore a  
7 material misrepresentation.

8           116. Upon information and belief, AT&T's security safeguards were  
9 inadequate, including its system which—upon information and belief—allowed an  
10 individual employee, representative and agent to conduct SIM swaps without  
11 adequate technical safeguards and oversight, even when that employee,  
12 representative and agent authorizes a COAM SIM swap over the phone in violation  
13 of company policy.

14           117. "Having one employee who can conduct these SIM swaps without any  
15 kind of oversight seems to be the real problem," says Lieutenant John Rose, a  
16 member of the California-based Regional Enforcement Allied Computer Team  
17 ("REACT"), a multi-jurisdictional law enforcement partnership specializing in  
18 cybercrime.<sup>95</sup> "And it seems like [the carriers] could really put a stop to it if  
19 there were more checks and balances to prevent that. It's still very, very easy to SIM  
20 swap, and something has to be done because it's just too simple. Someone needs to  
21 light a fire under some folks to get these protections put in place."

22           118. AT&T failed to put in place adequate systems and procedures to  
23 prevent the unauthorized employee, representative and agent access to and take  
24 over of Mr. Ross' account and related data. In connection with subsequent criminal  
25 investigations into Mr. Ross' SIM swap, AT&T informed law enforcement that it  
26 had the capacity to see how many different SIM cards had been associated with the

---

27  
28 <sup>95</sup> Busting SIM Swappers and SIM Swap Myths," KREBSONSECURITY (Nov. 18, 2018), *available*  
at <https://krebsonsecurity.com/2018/11/busting-sim-swappers-and-sim-swap-myths>.

1 same single mobile phone's IMEI.<sup>96</sup> In other words, AT&T could see when one  
2 mobile phone had multiple SIM cards associated with it in a short amount of time.<sup>97</sup>

3 119. AT&T also informed law enforcement that the hacker involved in Mr.  
4 Ross' SIM swap had requested that *eleven different phone numbers* be moved onto  
5 his phone (identified by its IMEI number) in the twenty-one days before Mr. Ross'  
6 swap.<sup>98</sup> The hacker sometimes moved three different AT&T numbers onto the same  
7 phone *in a single day*.<sup>99</sup> AT&T certainly had the capability to see this behavior, and  
8 could and should have flagged it as suspicious. If AT&T had proper security  
9 safeguards in place, it would have recognized this behavior, flagged it as suspicious,  
10 and prevented any further SIM swaps onto that phone – thereby protecting Mr.  
11 Ross.

12 120. Additionally, as alleged fully above, AT&T failed to establish a  
13 consent mechanism that verified proper authorization before Mr. Ross' data was  
14 accessed and provided to third parties. AT&T's statement that it would use  
15 encryption and other security safeguards to protect customers' data is therefore a  
16 material misrepresentation. AT&T easily and very quickly detected that the same  
17 phone was used in eleven prior unauthorized SIM swaps *before* the unauthorized  
18 SIM swap on Mr. Ross' phone, and gave this information to the REACT cybercrime  
19 task force.<sup>7</sup> However, AT&T did nothing to stop the hacker from using the same  
20 phone for multiple unauthorized SIM swaps, and had no voice biometric system or  
21 other solution in place to prevent the unauthorized SIM swaps.

22 121. AT&T's representation that it "will protect [customers'] privacy and  
23 keep [their] personal information safe" is false and misleading.

24 122. As alleged fully above, AT&T failed to establish a consent mechanism  
25 that verified proper authorization before Mr. Ross' account and the data therein

---

26 <sup>96</sup> Ex. B. at pp. 8, 22.

27 <sup>97</sup> *Id.*

28 <sup>98</sup> *Id.*

<sup>99</sup> *Id.* at 22.

were accessed and used without his authorization or consent and disclosed to third parties. Mr. Ross' privacy and personal information was not safe, as demonstrated by the breach of his AT&T account. AT&T's statement that it would protect customers' privacy and keep their personal information safe is therefore a material misrepresentation.

123. AT&T also makes numerous false or misleading representations concerning its treatment of customers' data that qualifies as CPNI under the FCA.

124. AT&T explicitly and falsely represents in its Privacy Policy that it does not "sell, trade or share" their CPNI:

We do not sell, trade or share your CPNI with anyone outside of the AT&T family of companies\* or our authorized agents, unless required by law (example: a court order).<sup>100</sup>

125. As alleged fully above, AT&T and its employees, representatives and agents provided access to Mr. Ross' CPNI to third-party hackers. This use was not required by law and was instead *prohibited* by law.

126. AT&T also states that it only uses CPNI "internally" and its *only* disclosed use of CPNI is "among the AT&T companies and our agents in order to offer you new or enhanced services."<sup>101</sup>

127. Defendants' employees', representatives' and agents' use of Mr. Ross' account and related data as described herein was not for "internal" AT&T purposes, nor was it used to market AT&T services. AT&T's statements regarding the use of customer CPNI are therefore material misrepresentations. Its failure to disclose this is a material omission.

---

<sup>100</sup> "Customer Proprietary Network Information (CPNI)," AT&T, Ex. C at 31-32. The "AT&T family of companies" is defined as "those companies that provide voice, video and broadband-related products and/or services domestically and internationally, including the AT&T local and long distance companies, AT&T Corp., AT&T Mobility, DIRECTV, and other subsidiaries or affiliates of AT&T Inc. that provide, design, market, or sell these products and/or services." *Id.*

<sup>101</sup> *Id.*

1           128. AT&T also falsely represents that it “uses technology and security  
2 features, and strict policy guidelines with ourselves and our agents, to safeguard the  
3 privacy of CPNI.”

4           129. As alleged fully above, AT&T and its agents failed to safeguard Mr.  
5 Ross’ CPNI. Instead, it stored customer CPNI in such a way that unauthorized  
6 access was easily obtained by employees and third parties. AT&T’s statements  
7 regarding the technology and security features it uses to safeguard customer CPNI  
8 are therefore material misrepresentations.

9           130. AT&T was obligated to disclose the weaknesses and failures of its  
10 account and data security practices, as AT&T had exclusive knowledge of material  
11 facts not known or knowable to its customers, AT&T actively concealed these  
12 material facts from Mr. Ross, and such disclosures were necessary to materially  
13 qualify its representations that it took measures to protect consumer data and to  
14 materially qualify its partial disclosures concerning its use of customers’ CPNI.  
15 Further, AT&T was obligated to disclose its practices under the FCA.

16           131. A reasonable person would be deceived and misled by AT&T’s  
17 misrepresentations, which clearly indicated that AT&T would safeguard its  
18 customers’ personal information and CPNI.

19           132. AT&T intentionally misled Mr. Ross regarding its data security  
20 practices in order to maintain his business, make money from his account, and  
21 evade prosecution for its unlawful acts. Furthermore, AT&T has invested millions  
22 into ZenKey to profit from the SIM swap problem, thereby incentivizing itself (and  
23 its two primary competitors) to not timely solve the problem to protect its  
24 customers, for which other carriers have implemented highly effective solutions.

25           133. AT&T’s representations that it protected customers’ personal  
26 information, when in fact it did not, were false, deceptive, and misleading and  
27 therefore a violation of the FCA.  
28



1     **VI. CLAIMS FOR RELIEF**

2  
3                     **COUNT I**

4             **Violations of The Federal Communications Act, 47 U.S.C. § 201 *et seq.***

5             134. Plaintiff Robert Ross realleges and incorporates all of the preceding  
6 paragraphs as though fully set forth in this cause of action.

7             135. Defendants have violated 47 U.S.C. § 222(a) by failing to protect the  
8 confidentiality of Mr. Ross' CPNI, as detailed herein.

9             136. Defendants have violated 47 U.S.C. § 222(c) by using, disclosing,  
10 and/or permitting access to Mr. Ross' CPNI without the notice, consent, and/or legal  
11 authorization required under the FCA, as detailed herein. Defendants also caused  
12 and/or permitted third parties to use, disclose, and/or permit access to Mr. Ross'  
13 CPNI without the notice, consent, and/or legal authorization required under the  
14 FCA, as detailed herein.

15             137. As fully alleged above, Mr. Ross has suffered injury to his person,  
16 property, health, and reputation as a consequence of Defendants' violations of the  
17 FCA. Additionally, Mr. Ross has suffered emotional damages, including severe  
18 anxiety and depression, mental anguish, and suffering as a result of Defendants' acts  
19 and practices. These emotional damages have led directly to physical issues; for  
20 example, Mr. Ross began stress-eating which resulted in Mr. Ross gaining  
21 approximately 40 pounds in only a few months following the Defendants-facilitated  
22 thefts.

23             138. Mr. Ross seeks the full amount of damages sustained as a  
24 consequence of Defendants' violations of the FCA, together with reasonable  
25 attorneys' fees, to be fixed by the Court and taxed and collected as part of the costs  
26 of the case. Mr. Ross also moves for a writ of injunction or other proper process,  
27 mandatory or otherwise, to restrain Defendants and their officers, agents, or  
28

1 representatives from further disobedience of the 2007 and 2013 CPNI Orders, or to  
2 compel their obedience to the same.

## 3 **COUNT II**

### 4 **Violations of The California Unfair Competition Law (“UCL”)** 5 **under the Unlawful, Unfair and Fraudulent Prongs,** 6 **California Business & Professional Code § 17200 *et seq.***

7 139. Plaintiff Robert Ross realleges and incorporates all of the preceding  
8 paragraphs as though fully set forth in this cause of action.

9 140. California’s Unfair Competition Law (UCL) prohibits any “unlawful,  
10 unfair or fraudulent business act or practice.” Defendants’ business acts and  
11 practices complained of herein were unlawful, unfair, and fraudulent.

12 141. AT&T made material misrepresentations and omissions concerning its  
13 safeguarding of Mr. Ross’ CPNI. As alleged fully above, a reasonable person  
14 would attach importance to the privacy of his sensitive account data in determining  
15 whether to contract with a mobile phone provider.

16 142. Defendants had a duty to disclose the nature of their inadequate  
17 security practices and failures in hiring, training, and supervising staff. Defendants  
18 had exclusive knowledge of material facts not known or knowable to AT&T  
19 customers and Defendants actively concealed these material facts from customers.

20 143. Further, additional disclosures were necessary to materially qualify  
21 AT&T’s representations that it did not sell consumer data and took measures to  
22 protect that data, and its partial disclosures concerning its use of customers’ CPNI.  
23 AT&T was obligated to disclose its practices, as required by the FCA. The  
24 magnitude of the harm suffered by Mr. Ross underscores the materiality of AT&T’s  
25 omissions.

26 144. A reasonable person, such as Mr. Ross, would be deceived and misled  
27 by AT&T’s misrepresentations, which indicated that Defendants would safeguard its  
28 customers’ personal and proprietary information.

1           145. AT&T intentionally misled its customers regarding its data protection  
2 practices in order to attract customers and evade prosecution for its unlawful acts.

3           146. Defendants' actions detailed herein constitute an unlawful business act  
4 or practice. As alleged herein, Defendants' conduct is a violation of the California  
5 constitutional right to privacy and the FCA.

6           147. Defendants' actions detailed herein constitute an unfair business act or  
7 practice.

8           148. Defendants' conduct lacks reasonable and legitimate justification in  
9 that Mr. Ross has been misled as to the nature and integrity of AT&T's goods and  
10 services and has suffered injury as a result.

11           149. The gravity of the harm caused by Defendants' practices far outweigh  
12 the utility of their conduct. Defendants' practices were contrary to the letter and  
13 spirit of the FCA and its corresponding regulations, which require mobile carriers to  
14 disclose customers' CPNI only upon proper notice, consent, and authorization, and  
15 aims to vest carrier customers with control over their data. Due to the surreptitious  
16 nature of Defendants' actions, Mr. Ross could not have reasonably avoided the  
17 harms incurred as a result.

18           150. As the FCA establishes, it is against public policy to allow carrier  
19 employees or other third parties to access, use, or disclose telecommunications  
20 customers' sensitive account information. The effects of Defendants' conduct are  
21 comparable to or the same as a violation of the FCA.

22           151. Defendants' actions detailed herein constitute a fraudulent business  
23 act or practice.

24           152. As established herein, Mr. Ross has suffered injury in fact and  
25 economic harm as a result of AT&T's unfair competition. Additionally, had  
26 Defendants disclosed the true nature and extent of their data security and protection  
27 practices—and the flaws inherent in their systems—and their unwillingness to  
28

1 properly protect its customers, Mr. Ross would not have subscribed to or paid as  
2 much money for AT&T's mobile services.

3 153. Mr. Ross seeks injunctive and declaratory relief for Defendants'  
4 violations of the UCL. Mr. Ross seeks public injunctive relief against Defendants'  
5 unfair and unlawful practices in order to protect the public and restore to the parties  
6 in interest money or property taken as a result of Defendants' unfair competition.  
7 Mr. Ross seeks a mandatory cessation of Defendants' practices, and proper  
8 safeguarding of AT&T account data.

### 9 **COUNT III**

#### 10 **Violations of the California Constitutional Right to Privacy**

11 154. Plaintiff Robert Ross realleges and incorporates all of the preceding  
12 paragraphs as though fully set forth in this cause of action.

13 155. The California Constitution declares that, "All people are by nature  
14 free and independent and have inalienable rights. Among these are enjoying and  
15 defending life and liberty, acquiring, possessing, and protecting property, and  
16 pursuing and obtaining safety, happiness, and privacy." Cal. Const. Art. I, § 1.

17 156. Mr. Ross has a reasonable expectation of privacy in his mobile device  
18 and his AT&T account information.

19 157. Defendants intentionally intruded on and into Mr. Ross' solitude,  
20 seclusion, or private affairs by allowing its employees and third parties to  
21 improperly access Mr. Ross' confidential AT&T account information without proper  
22 consent or authority.

23 158. The reasonableness of Mr. Ross' expectations of privacy is supported  
24 by AT&T and its agents' unique position to safeguard his account data, including  
25 the sensitive and confidential information contained therein, and protect Mr. Ross  
26 from SIM swap attacks.

27 159. AT&T and its agents' intrusions into Mr. Ross' privacy are highly  
28 offensive to a reasonable person. This is evidenced by federal legislation enacted

1 by Congress and rules promulgated and enforcement actions undertaken by the FCC  
2 aimed at protecting AT&T customers' sensitive account data from unauthorized use  
3 or access.

4 160. The offensiveness of Defendants' conduct is heightened by AT&T's  
5 material misrepresentations to Mr. Ross concerning the safety and security of his  
6 account.

7 161. Mr. Ross suffered great personal and financial harm by the intrusion  
8 into his private affairs, as detailed throughout this Complaint.

9 162. Defendants' actions and conduct complained of herein were a  
10 substantial factor in causing the harm suffered by Mr. Ross. But for Defendants'  
11 agents' and employees' unauthorized access to Mr. Ross' account and AT&T's  
12 failure to protect Mr. Ross from such harm through adequate security and oversight  
13 systems and procedures, Mr. Ross would not have had his personal privacy  
14 repeatedly violated and would not have been a victim of SIM swap theft resulting in  
15 his loss of \$1,000,000 in cash and the breach of sensitive personal information.

16 163. As a result of Defendants' actions, Mr. Ross seeks nominal and  
17 punitive damages in an amount to be determined at trial. Mr. Ross seeks punitive  
18 damages because Defendants' actions were malicious, oppressive, and willful.  
19 Defendants knew or should have known about the risks faced by Mr. Ross, and the  
20 grave consequences of such risks. Nonetheless, Defendants utterly failed to protect  
21 Mr. Ross, and instead, AT&T has invested millions of dollars into a scheme to profit  
22 from SIM swaps through ZenKey. Punitive damages are warranted to deter  
23 Defendants from engaging in future misconduct.

24  
25 **COUNT IV**  
26 **Negligence**

27 164. Plaintiff Robert Ross realleges and incorporates all of the preceding  
28 paragraphs as though fully set forth in this cause of action.

1           165. Defendants owed a duty to Mr. Ross—arising from the sensitivity of  
2 his AT&T account information and the foreseeability of harm to Mr. Ross should  
3 Defendants fail to safeguard and protect such data—to exercise reasonable care in  
4 safeguarding his sensitive personal information. This duty included, among other  
5 things, designing, maintaining, monitoring, and testing AT&T’s and its agents’,  
6 partners’, and independent contractors’ systems, protocols, and practices to ensure  
7 that Mr. Ross’ information was adequately secured from unauthorized access.

8           166. Federal law and regulations, as well as AT&T’s privacy policy,  
9 acknowledge Defendants’ duty to adequately protect Mr. Ross’ confidential account  
10 information.

11           167. Defendants owed a duty to Mr. Ross to protect his sensitive account  
12 data from unauthorized use, access, or disclosure. This included a duty to ensure  
13 that his CPNI was used, accessed, or disclosed only with proper consent.

14           168. Defendants owed a duty to Mr. Ross to implement a system to  
15 safeguard against and detect unauthorized access to Mr. Ross’ AT&T data in a  
16 timely manner.

17           169. Defendants owed a duty to Mr. Ross to disclose the material fact that  
18 their data security practices were inadequate to safeguard Mr. Ross’ AT&T account  
19 data from unauthorized access by its own employees and others.

20           170. AT&T had a special relationship with Mr. Ross due to its status as his  
21 telecommunications carrier, which provided an independent duty of care. AT&T  
22 had the unique ability to protect its systems and the data it stored thereon from  
23 unauthorized access.

24           171. Mr. Ross’ willingness to contract with AT&T, and thereby entrust  
25 AT&T with his confidential and sensitive account data, was predicated on the  
26 understanding that AT&T and its agents would undertake adequate security and  
27 consent precautions.

1           172. Defendants breached their duties by, *inter alia*: (a) failing to  
2 implement and maintain adequate security practices to safeguard Mr. Ross' AT&T  
3 account and data—including his CPNI—from unauthorized access, as detailed  
4 herein; (b) failing to detect unauthorized accesses in a timely manner; (c) failing to  
5 disclose that their data security practices were inadequate to safeguard Mr. Ross'  
6 data; (d) failing to supervise their agents and employees and prevent them from  
7 accessing and utilizing Mr. Ross' AT&T account and data without authorization;  
8 and (e) failing to provide adequate and timely notice of unauthorized access.

9           173. Defendants were also negligent in their authorization of Mr. Ross'  
10 SIM card swap. Defendants knew or should have known that at least ten different  
11 AT&T numbers had been moved to the same mobile phone (identified by its IMEI)  
12 in the weeks leading up to Mr. Ross' SIM swap. Defendants knew or should have  
13 known that this was highly suspicious. Nevertheless, Defendants effectuated the  
14 transfer of Mr. Ross' AT&T account to this same mobile phone. Defendants had the  
15 technical capacity to track this behavior—as reflected in its willingness to do so  
16 quickly for law enforcement—but nonetheless failed to utilize it for the benefit and  
17 protection of Mr. Ross.

18           174. But for Defendants' breaches of their duties, Mr. Ross' data would not  
19 have been accessed by unauthorized individuals.

20           175. Mr. Ross was a foreseeable victim of Defendants' inadequate data  
21 security practices and consent mechanisms. As alleged fully above, AT&T and its  
22 agents knew or should have known that SIM swaps presented a serious threat to its  
23 customers, including Mr. Ross, before Mr. Ross' account was breached for the first  
24 time. Defendants also knew or should have known that improper procedures and  
25 systems to safeguard customer data could allow their agents and employees to  
26 authorize customers' accounts and data, as occurred in the 2015 FCC enforcement  
27 action.  
28



1           176. Defendants knew or should have known that unauthorized access  
2 would cause damage to Mr. Ross. AT&T admitted that unauthorized account access  
3 presents a significant threat to its customers, and it became aware during its 2015  
4 FCC enforcement action of the harms caused by unauthorized account access.

5           177. Defendants' negligent conduct provided a means for unauthorized  
6 individuals to access Mr. Ross' AT&T account data, take over control of his mobile  
7 phone, and use such access to hack into numerous online accounts in order to rob  
8 Mr. Ross and steal his personal information. As a result of Defendants' failure to  
9 prevent unauthorized accesses, Mr. Ross suffered grave injury, as alleged fully  
10 above, including severe emotional distress. This emotional distress arose out of  
11 Defendants' breach of their legal duties. The damages Mr. Ross suffered were a  
12 proximate, reasonably foreseeable result of Defendants' breaches of their duties.  
13 Therefore, Mr. Ross is entitled to damages in an amount to be proven at trial.

14           178. The injury and harm suffered by Mr. Ross was the reasonably  
15 foreseeable result of AT&T's failure to exercise reasonable care in safeguarding and  
16 protecting Mr. Ross's Personal Information, including his CPI and CPNI. AT&T's  
17 misconduct as alleged herein is malice, fraud or oppression under Civil Code §  
18 3294(c)(1) and (2) in that it was despicable conduct carried on by AT&T with a  
19 willful and conscious disregard of the rights or safety of Mr. Ross and despicable  
20 conduct that has subjected Mr. Ross to cruel and unjust hardship in conscious  
21 disregard of his rights. As a result, Mr. Ross is entitled to punitive damages against  
22 AT&T under Civil Code § 3294(a). Mr. Ross further alleges on information and  
23 belief that Bill O'Hern, who has been in charge of security at AT&T since 2016, and  
24 David S. Huntley, who has been in charge of privacy, had advance knowledge of the  
25 inadequacies of AT&T's security, the participation of AT&T employees in evading  
26 or bypassing security, and they committed or ratified the acts of oppression, fraud or  
27 malice alleged herein.  
28

**COUNT V**  
**Concealment**

179. Plaintiff Robert Ross realleges and incorporates all of the preceding paragraphs as though fully set forth in this cause of action.

180. As alleged above, AT&T, including Chief Security Officer Bill O'Hern and Chief Compliance Officer David S. Huntley, who are respectively in charge of AT&T's security and privacy protections, knew that its data security measures were grossly inadequate, that its employees and agents could readily bypass the procedures, that its employees actively cooperated with hackers and thieves, and that it was incapable of living up to its commitments to consumers, including to Mr. Ross, under state and federal law, as well as under its own Privacy Policy, to protect his Personal Information, including CPI and CPNI.

181. Mr. Ross was unaware that AT&T's security measures did not include low cost and readily available solutions which would have prevented his SIM swap and resulting theft.

182. AT&T, including Mr. O'Hern and Mr. Huntley, knew or should have known from prior incidents and contacts with law enforcement that its system was subject to SIM swap fraud, that its employees cooperated with hackers in such fraud, that such fraud was prevalent in the cryptocurrency community, and that its security measures were ineffective in preventing the fraud. Mr. O'Hern should have been well aware of this because he is in charge of security and AT&T and Mr. Huntley should have known because he is in charge of insuring that AT&T protects the privacy of its customers.

183. AT&T did not disclose these things to Mr. Ross and willfully deceived Mr. Ross by concealing the true facts concerning its data security, which AT&T was legally obligated and had a duty to disclose. It did so in order to induce Mr. Ross to remain as its customer.

184. Had AT&T disclosed the true facts about its dangerously poor data

1 security practices and that is was motivated to profit from SIM swaps rather than  
2 correct the problem, Mr. Ross would have taken further measures to protect himself  
3 and would have ceased being a customer of AT&T.

4 185. Mr. Ross justifiably relied on AT&T to provide accurate and complete  
5 information about its data security in continuing to be AT&T's customer. Rather  
6 than disclosing the inadequacies in its security, including the additional security it  
7 encouraged Mr. Ross to place on his account, AT&T willfully suppressed any  
8 information relating to such inadequacies.

9 186. AT&T's actions are "deceit" under Cal. Civ. Code § 1710 in that they  
10 are the suppression of a fact by one who is bound to disclose it, or who gives  
11 information of other facts which are likely to mislead for want of communication  
12 of that fact Because of the deceit by AT&T, it is liable under Cal. Civ. Code§ 1709  
13 for "any damage which [Mr. Ross] thereby suffers."

14 187. Because of this deceit by Defendants, Mr. Ross's Personal  
15 Information, including his CPI and CPNI, as described above, was compromised  
16 by hackers and he was deprived of \$1 million. The connection between AT&T, the  
17 SIM swap and the loss of Mr. Ross's funds is alleged hereinabove. In addition, Mr.  
18 Ross's Personal Information is now easily available to hackers, including through  
19 the Dark Web. Mr. Ross is further damaged to the extent of the amounts that he has  
20 paid AT&T for wireless services, because those services were either worth nothing  
21 or worth less than was paid for them because of lack of security. Mr. Ross has also  
22 suffered substantial out-of-pocket costs because of AT&T's inadequate security.

23 188. Because AT&T's deceit is fraud under Civil Code § 3294(c)(3) ,and  
24 AT&T's conduct was done with malice, fraud and oppression, Mr. Ross is entitled  
25 to punitive damages under Civil Code § 3294(a). Mr. Ross further alleges on  
26 information and belief that Bill O'Hern, who has been in charge of security at  
27 AT&T since 2016, and David S. Huntley, who has been in charge of privacy, had  
28 advance knowledge of the inadequacies of AT&T's security, the participation of

1 AT&T employees in evading or bypassing security, and they committed or ratified  
2 the acts of oppression, fraud or malice alleged herein.

3  
4 **COUNT VI**  
5 **Negligent Supervision and Entrustment**

6 189. Plaintiff Robert Ross realleges and incorporates all of the preceding  
7 paragraphs as though fully set forth in this cause of action.

8 190. AT&T conducts its business activities through employees or other  
9 agents, including One Touch Direct and One Touch Direct-SA.

10 191. Defendants are liable for harm resulting from their agents and  
11 employees because they were reckless or negligent in employing and/or entrusting  
12 agents and employees in work involving the risk of harm to others, including Mr.  
13 Ross.

14 192. On information and belief, Defendants knew or had reason to believe  
15 that their agents and employees were unfit and failed to exercise reasonable care in  
16 properly investigating and overseeing them. AT&T was negligent in supervising its  
17 agents and in entrusting them with what it knew to be highly sensitive confidential  
18 information. One Touch Direct and One Touch Direct-SA were negligent in  
19 supervising their agents and employees and in entrusting them with what they knew  
20 to be highly sensitive confidential information. Defendants knew or had reason to  
21 know that their agents and employees were likely to harm others in view of the  
22 work AT&T entrusted to them. Specifically, AT&T entrusted its agents and  
23 employees with the responsibility to conduct SIM card changes without sufficient  
24 oversight – as demonstrated by the representative and agent effectuating the  
25 October 2018 SIM swap on Mr. Ross' account despite AT&T's policy disallowing  
26 COAM SIM changes over the phone.

27 193. Additionally, as alleged fully above, the hacker involved in Mr. Ross'  
28 SIM swap had associated numerous different SIM cards with the same device IMEI

1 in the days leading up to Mr. Ross' attack. Despite the highly suspicious nature of  
2 this activity, and AT&T's ability to track such requests, AT&T and its agents failed  
3 to put any additional protections on customer accounts to prevent its employees  
4 from approving additional SIM swaps to the same IMEI.

5 194. Upon information and belief, Defendants failed to exercise due care in  
6 selecting their agents and employees, and thereby negligently or recklessly  
7 employed employees to do acts—including accessing customer accounts and  
8 effectuating SIM swaps—which necessarily brought them in contact with others,  
9 including Mr. Ross, while in the performance of those duties.

10 195. Defendants' acts, as alleged herein, were negligent in that they created  
11 the risk of unauthorized account access, SIM card changes, and the damages  
12 resulting therefrom.

13 196. Defendants also failed to properly supervise their agents and  
14 employees, and instead continued to negligently entrust them with sensitive  
15 customer data. On information and belief, had AT&T not contracted out customer  
16 service functions to third parties such as One Touch Direct and One Touch Direct-  
17 SA, and had One Touch Direct or One Touch Direct-SA fired the involved the  
18 employee when they first began to exhibit suspicious SIM swap activity—including  
19 but not limited to approving SIM changes that violated AT&T policy—Mr. Ross  
20 would not have been injured.

21 197. On information and belief, had Defendants built a system to  
22 effectively authenticate and verify consumer consent before allowing its agents or  
23 employees to access their CPNI—as required by the FCA—Mr. Ross would not  
24 have been injured.

25 198. On information and belief, had Defendants prevented individual  
26 employees from unilaterally performing SIM swaps without proper oversight, Mr.  
27 Ross would not have been injured.

1           199. In sum, Defendants gave their agents and employees the tools and  
2 opportunities they needed to gain unauthorized access to Mr. Ross' account and  
3 failed to prevent them from doing so, thereby allowing them to use AT&T's systems  
4 to perpetuate privacy breaches and thefts against Mr. Ross.

5           200. The Defendants' agent(s') and employee(s') actions have a causal  
6 nexus to their employment. Mr. Ross' injuries arose out of his contract with AT&T  
7 as his carrier, and AT&T's access to his CPNI and account data as a result. The risk  
8 of injury to Mr. Ross was inherent in the AT&T working environment.

9           201. Mr. Ross' injury was also foreseeable. As alleged fully above,  
10 Defendants were aware of the risks that SIM swaps presented to AT&T customers.  
11 Defendants were also aware that AT&T customers' accounts were vulnerable to  
12 unauthorized access by their agents and employees, as demonstrated in the 2015  
13 FCC enforcement action. Furthermore, Mr. Ross' injury was foreseeable as  
14 Defendants could have and should have seen that the same hacker phone had been  
15 used in multiple previous unauthorized SIM swaps.

## 16 17 **COUNT VII**

### 18 **Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030**

19           202. Plaintiff Robert Ross realleges and incorporates all of the preceding  
20 paragraphs as though fully set forth in this cause of action.

21           203. Mr. Ross' mobile device is capable of connecting to the Internet.

22           204. Defendants' agents and employees, in the scope of their employment,  
23 intentionally accessed Mr. Ross' mobile device, and assisted others in accessing his  
24 mobile device, without Mr. Ross' authorization, in order to assist hackers in their  
25 theft of Mr. Ross.

26           205. The Defendants agents and employees took these actions knowing  
27 that they would cause damage to Mr. Ross' mobile device, as well as damage to the  
28 information located on his mobile device.

1           206. The Defendants agents and employees caused Mr. Ross' mobile  
2 device and much of the data on it to be unusable to him.

3           207. Because of the Defendants' agents' and employees' actions, Mr. Ross  
4 suffered damage to his mobile device and damage to information on his mobile  
5 device, including being unable to access information and data on his mobile device  
6 and being unable to access his personal accounts, including his personal (e.g.  
7 Gmail) and financial (e.g. cryptocurrency and PayPal) accounts.

8           208. The act of swapping Mr. Ross' AT&T mobile SIM card was in the  
9 scope of the Defendants' agents and employees' work.

10          209. Further, Mr. Ross spent in excess of \$5,000 investigating who  
11 accessed his mobile device and damaged information on it.  
12

## 13       **VII. PRAYER FOR RELIEF**

14          210. WHEREFORE, Plaintiff Robert Ross requests that judgment be  
15 entered against Defendants and that the Court grant the following:

- 16           A. Judgment against Defendants for Plaintiff's asserted causes of action;
- 17           B. Public injunctive relief requiring cessation of Defendants' acts and  
18 practices complained of herein pursuant to, *inter alia*, Cal. Bus. &  
19 Prof. Code § 17200 and 47 U.S.C. § 401(b);
- 20           C. Pre- and post-judgment interest, as allowed by law;
- 21           D. An award of monetary damages, including punitive damages, as  
22 allowed by law;
- 23           E. Reasonable attorneys' fees and costs reasonably incurred, including  
24 but not limited to attorneys' fees and costs pursuant to 47 U.S.C. §  
25 206; and
- 26           F. Any and all other and further relief to which Plaintiff may be entitled.  
27  
28



**DEMAND FOR JURY TRIAL**

Plaintiff demands a trial by jury of all issues so triable.

DATED:

CHRISTOPHER GRIVAKES  
AFFELD GRIVAKES LLP

By: /s/ DRAFT

Christopher Grivakes

Attorneys for Plaintiff ROBERT ROSS